Multi-Function Wireless Router

Wireless Access Point

Broadband Internet Access

Dial-in RAS

Print Server

User's Guide

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 1
- Wireless Router Features 1
- Package Contents 4
- Physical Details 4

CHAPTER 2 INSTALLATION 7
- Requirements 7
- Procedure 7

CHAPTER 3 CONFIGURATION 9
- Overview 9
- Configuration Program 10
- Quick Setup Screen 12
- Wireless Screen 16
- Status Screen 19

CHAPTER 4 PC CONFIGURATION 25
- Overview 25
- Windows Clients 25
- Macintosh Clients 36
- Linux Clients 37
- Other Unix Systems 38
- Wireless Station Configuration 38

CHAPTER 5 DHCP 39
- Overview 39
- What DHCP Does 39
- Using the Wireless Router's DHCP Server 39
- Using another DHCP Server 39
- To Configure your PCs to use DHCP 40

CHAPTER 6 SERIAL PORT 41
- Overview 41
- Serial Port Screen 41
- Modem Properties Screen 44
- Dial -in Users 46
- Serial Port Status 50

CHAPTER 7 OPTIONS 53
- Overview 53
- Password 53
- DNS (Domain Name Server 54
- NAT (Network Address Translation) 54
- TFTP 54
- Remote Management 54
- Routing Table 55
- Printer Port 55

CHAPTER 8 ROUTING 57
- Overview 57
- Routing Screen 57
- Router Configuration 59
- Static Routing - Example 60

CHAPTER 9 ADVANCED INTERNET 61
- Overview 61
- Advanced Internet Screen 61
- Special Internet Applications 62

URL Filter **65**
Virtual Servers **67**
DMZ **72**
CHAPTER 10 ACCESS CONTROL **74**
Overview **74**
Security Groups Screen **75**
PCs Screen **77**
Filters Screen **79**
APPENDIX A TROUBLESHOOTING **80**
Overview **80**
General Problems **80**
Internet Access **80**
Wireless Access **81**
Printing **82**
Dial-in Access **85**
APPENDIX B ABOUT WIRELESS LANS **88**
Modes **88**
BSS/ESS **88**
Channels **89**
WEP **89**
Access Control **90**
Wireless LAN Configuration **90**
APPENDIX C AT COMMANDS **91**
AT Commands **91**
Standard AT Commands **93**
APPENDIX D SPECIFICATIONS **96**
Multi-Function Wireless Router **96**
PCMCIA Wireless Card **97**

P/N: 9560DP0001

Copyright © 2001. All Rights Reserved.

Document Version: 1.0

All trademarks and trade names are the properties of their respective owners.

Chapter 1
Introduction

This Chapter provides an overview of the Wireless Router's features and capabilities.

Congratulations on the purchase of your new Wireless Router Multi-Function Wireless Router. The Wireless Router is a multi-function device providing the following services:

- **Shared Internet Access** via an DSL or Cable modem on the WAN (Ethernet) port, OR via an analog modem or ISDN TA on the Serial (RS232) port.
- **Wireless LAN Access Point** (base station) for equipment compliant with the IEEE802.11b (DSSS) specifications.
- **Network Printer** - LAN and WLAN users can share the printer attached to the Wireless Router.
- **RAS Dial-in Access** - Remote users can use the Wireless Router to connect to the LAN and access LAN resources, including the Wireless Router's printer and Broadband Internet access.

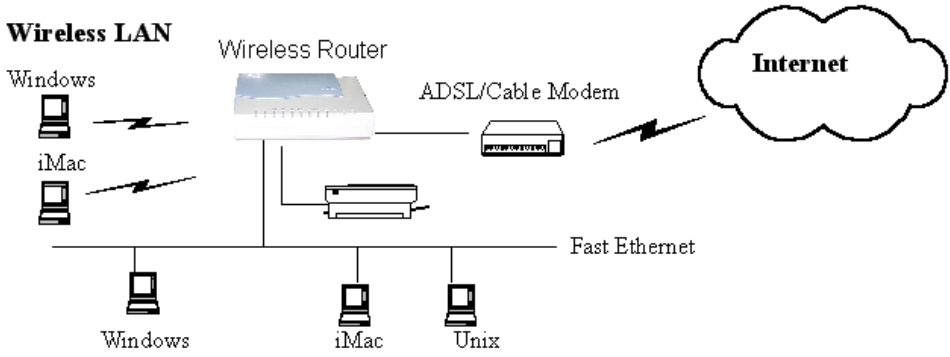


Figure 1: Wireless Router

Wireless Router Features

The Wireless Router incorporates many advanced features, carefully designed to provide sophisticated functions while being easy to use.

LAN Features

- ***Dual LAN ports.*** The Wireless Router has two (2) 10/100BaseT Ethernet LAN ports. Normally, the "Hub" port is used to connect the Wireless Router to a 10/100BaseT hub on your LAN. But if desired, the "PC" port can be used to connect the Wireless Router directly to your PC, using a standard LAN cable.
- ***DHCP Server Support.*** **D**ynamic **H**ost **C**onfiguration **P**rotocol provides a dynamic IP address to PCs and other devices upon request. The Wireless Router can act as a **DHCP Server** for devices on your local LAN and WLAN.
- ***Multi Segment LAN Support.*** LANs containing one or more segments are supported, via the Wireless Router's built-in static routing table. If NAT (Network Address Translation) is disabled, the Wireless Router will function as a static router.

Internet Access Features

- ***Shared Internet Access.*** All users on the LAN or WLAN can access the Internet through the Wireless Router, using only a single external IP Address. The local (invalid) IP Addresses are hidden from external sources. This process is called NAT (Network Address Translation).
- ***DSL & Cable Modem Support.*** The Wireless Router has a 10BaseT Ethernet port for connecting an DSL or Cable Modem. All popular DSL and Cable Modems are supported.
- ***Analog Modem and ISDN TA Support.*** If you don't yet have Broadband Internet access, the Wireless Router can provide shared Internet access via an analog modem or ISDN TA connected to the serial (RS232) port.
- ***PPPoE Support.*** The WAN port connection can use PPPoE (PPP over Ethernet), if your ISP uses this method.
- ***Fixed or Dynamic IP Address.*** On the WAN connection, the Wireless Router supports both Dynamic IP Address (IP Address is allocated on connection) and Fixed IP Address.

Wireless Features

- ***Standards Compliant.*** The Wireless Router complies with the IEEE802.11b (DSSS) specifications for Wireless LANs.
- ***Security Features.*** Support for WEP (Wired Equivalent Privacy) and Access Control is included.
- ***Simple Configuration.*** If the default settings are unsuitable, they can be changed quickly and easily.

Network Printer

- ***Share your Printer.*** A printer connected to the Wireless Router's parallel port can be used by all PCs on the LAN.
- ***Multiple Operating Systems.*** Clients may use any of the following operating systems:
  - Windows 95/98/ME
  - Windows NT 4.0 or 2000
  - Apple Macintosh
  - Unix
- ***Multi--protocol Support.*** The following printing methods are supported:
  - Windows peer-to-peer printing over TCP/IP, using the supplied port driver.
  - Windows LPD printing, using a Windows Server running NT 4.0 or Windows 2000 Server. In this situation, no software needs to be installed on the client PCs.
  - Unix LPD printing. No additional software needs to be installed.

Advanced Internet Functions

- ***Virtual Servers.*** This feature allows Internet users to access Internet servers on your LAN. The required setup is quick and easy.
- ***User-Defined Virtual Servers.*** Internet users can access non-standard Internet Servers on your LAN by using this feature.

- ***Special Internet Applications.*** Internet applications such as Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers are supported.
- ***DMZ.*** One (1) PC on your local LAN can be configured to allow unrestricted 2-way communication with Servers or individual users on the Internet.
- ***URL Filter.*** Use the URL Filter to block access to undesirable Web sites by LAN users, Wireless LAN users, or the Dial-in user.
- ***Internet Access Log.*** See which Internet connections have been made.

RAS (Remote Access Services)

- ***RAS Dial-in.*** Remote PC users can use their standard Dial-up software to connect to the Wireless Router and access LAN resources.
- ***Dial-back Support.*** For additional security, the Dial-back feature can be used to hang up and re-dial the remote user. Both fixed and roaming options are supported.

Configuration & Management

- ***Easy Setup.*** Use your WEB browser from anywhere on the LAN for configuration.
- ***Remote Management.*** The Wireless Router can be managed from any PC on your LAN. And, if the Internet connection exists, it can also (optionally) be configured via the Internet.

Security Features

- ***Configuration Data***. Optional password protection is provided to prevent unauthorized users from modifying the configuration.
- ***Access Control Features***. The LAN Administrator can limit Internet access by individual workstations. And the *Access Control* log allows the Administrator to see attempted accesses which have been blocked.
- ***Wireless LAN Security***. WEP (Wired Equivalent Privacy) is supported, as well as Wireless access control via station address.
- ***Firewall Protection.*** All incoming data packets are monitored and all incoming server requests are filtered, thus protecting your network from malicious attacks from external sources. (This protection is lost if NAT is disabled.)

NAT Firewall Protection

The firewall protection provided by the Wireless Router is an intrinsic side effect of NAT (Network Address Translation). All users on the LAN share a single external IP address. From the external viewpoint, there is no network, only a single device.

For internal users, the Wireless Router acts as a “transparent proxy server”, translating the multiple internal IP addresses into a single external IP address.

For external requests, any attempt to connect to local resources is blocked. The Wireless Router will not “reverse translate” from a external IP address to a local IP address.

This type of “natural” firewall provides an impregnable barrier against malicious attacks.

Package Contents

The following items should be included:

- The Wireless Router Unit
- Wireless PCMCIA Card
- Power Adapter
- Quick Installation Guide
- CD-ROM containing the on-line manual and Print Port Driver.

If any of the above items are damaged or missing, please contact your dealer immediately.

Physical Details

Top-mounted LEDs

Power	**On** - Power on.
	Off - No power.
Status (Red)	**On** - Error condition.
	Off - Normal operation.
	Blinking - This LED blinks during start up.
WAN	**On** - WAN connection is established.
	Flashing - Data is being transmitted or received via the WAN port.
LAN: 10	**On** - LAN connection is using 10BaseT.
	Off - No LAN connection.
	Flashing - Data is being transmitted or received via the LAN port.
LAN: 100	**On** - LAN connection is using 100BaseT.
	Off - No LAN connection.
	Flashing - Data is being transmitted or received via the LAN port.
Wireless	**On** - Wireless connection available; Wireless Access Point is ready for use.
	Off - No Wireless connection available.
	Flashing - Data is transmitted or received via the Wireless access point. This includes "network traffic" as well as user data.
Print Error	**On** - Printer error detected.
	Off - No printer error detected.
Print Act	**On** - Connection to printer established.
	Off - No connection to printer; printer is Off or Off-line.
	Flashing - Data is being transmitted to the printer.
COM	**Off** - Idle or no active device connected to the serial (RS232) port.
(Serial Port)	**Flashing** - Data is transmitted or received via the serial (RS232) port.

Rear Panel

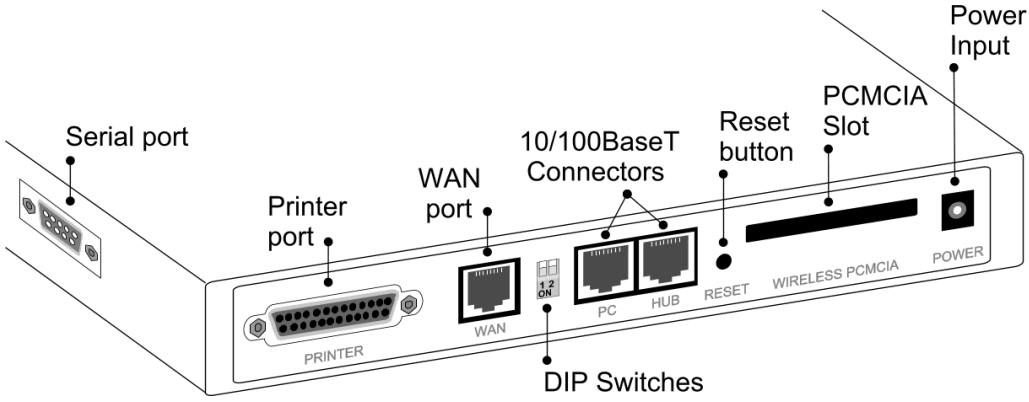


Figure 2: Rear Panel

Serial Port	RS232 Serial Port. If you have an analog modem or ISDN TA, connect it here.
Printer Port	Standard parallel printer port. If you wish to share a printer, connect it here.
WAN port (10BaseT)	Connect the DSL or Cable Modem here. If your modem came with a cable, use the supplied cable. Otherwise, use a standard LAN cable.
DIP switches	Refer to the following table.
PC port (10/100BaseT)	If connecting directly to your PC (no Hub) use this port and a standard LAN cable (RJ45 connectors). **Use EITHER the PC port OR the Hub port, NOT both.**
HUB port (10/100BaseT)	Use a standard LAN cable (RJ45 connectors) to connect this port to a 10BaseT or 100BaseT hub. **Use EITHER the PC port OR the Hub port, NOT both.**

Reset Button	This button has three (3) functions:
	• **Reboot**. When pressed and released, the Wireless Router will reboot (restart).
	• **Diagnostic print-out**. If held down for 3 seconds, a diagnostic print-out will be sent to the attached printer.
	  • Ensure the printer is ready.
	  • Both *Print* LEDs will flash simultaneously during the diagnostic printing.
	• **Clear All Data**. This button can also be used to clear ALL data and restore ALL settings to the factory default values.
	To Clear All Data and restore the factory default values:
	1. Power Off.
	2. Hold the Reset Button down while you Power On.
	3. Keep holding the Reset Button for a few seconds, until the RED LED has flashed TWICE.
	4. Release the Reset Button. The Wireless Router is now using the factory default values.

PCMCIA slot Insert the supplied Wireless PCMCIA card into this slot.

- ***Ensure the power is OFF before inserting or removing the PCMCIA Card.***
- ***Do not use any other PCMCIA Card.***

Power port (12V) Connect the supplied power adapter here.

DIP Switches

DIP Switch Setting	Description
1=off 2=off	Normal Operation.
1=off 2=on	DHCP Server function disabled.
1=on 2=off	Used to restore Default IP Address and clear Password (See below).
1=on 2=on	Normal Operation.

Restore Default IP Address and Clear Password

If the Wireless Router's IP Address or password is lost, the following procedure can be used to recover from this situation.

1. Turn the power to the Wireless Router OFF.
2. Set DIP switch 1 ON.
3. Turn the power to the Wireless Router ON.
4. Operate DIP switch 1 in the following sequence (you have 15 seconds to complete the sequence):
   - OFF
   - ON
   - OFF
5. The Wireless Router will now reset, and the Red Status LED flash. The following changes will have been made. (Other configuration data is unchanged.)
   - *IP Address* set to its default value of 192.168.0.1
   - *Network Mask* set to 255.255.255.0
   - *DHCP Server* is enabled, and will allocate IP Addresses in the range 192.168.0.2 to 192.168.0.51.
   - The password cleared (no password).
6. You can now connect to the Wireless Router and make any configuration changes required.

Chapter 2
Installation

This Chapter covers the physical installation of the Wireless Router.

Requirements

- Ethernet LAN (10/100BaseT) and the TCP/IP protocol.
- For Internet Access, an Internet Access account with an ISP, and either of:
  - A DSL or Cable modem (for WAN port usage)
  - An analog modem or ISDN TA (for serial port usage)
- To use the Wireless Access Point, all Wireless devices must be compliant with the IEEE802.11b specifications.
- For shared access to the attached printer, the following clients are supported:
  - Windows 95/98/ME
  - Windows NT 4.0 or 2000
  - Apple Macintosh
  - Unix (LPD printing)

Procedure

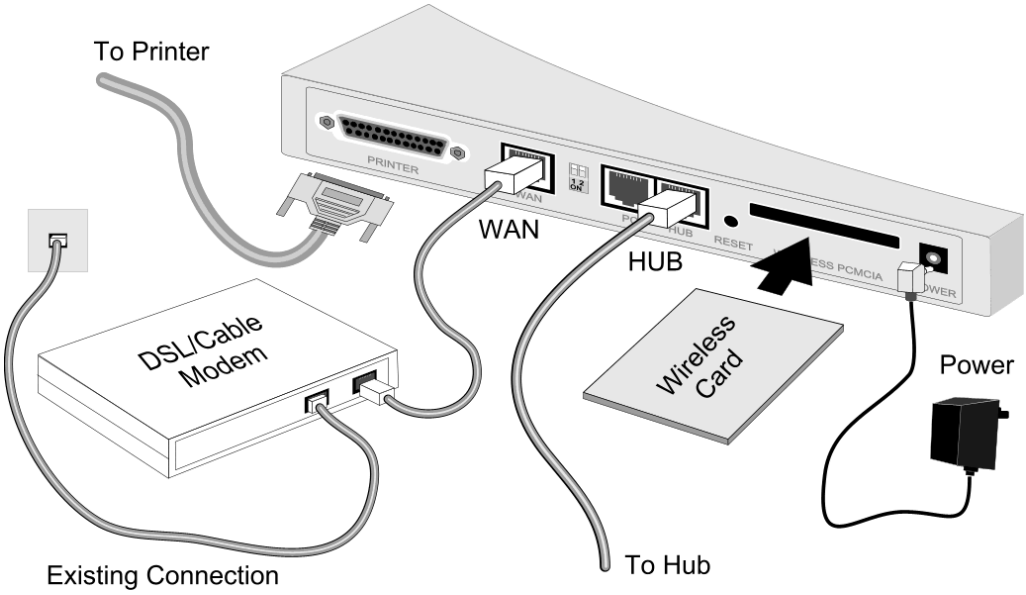


Figure 3: Installation Diagram

1. Choose an Installation Site

Select a suitable physical location. Ensure the Wireless Router and the DSL/Cable modem are powered OFF.

2. Insert Wireless PCMCIA card

Ensuring the supplied Wireless PCMCIA card is the right way up, insert it into the slot on the rear. Push it firmly until it clicks into position.

3. Connect LAN Cable

Connect a standard LAN cable from a 10BaseT or 100BaseT Hub on your LAN to the "HUB" port on the Wireless Router.

4. Connect WAN Cable

If you have a DSL modem or Cable modem, connect it to the WAN port on the Wireless Router. Use the cable supplied with your modem. If no cable was supplied, use a standard LAN cable.

5. Connect Modem (optional)

If you wish to use an Analog modem or ISDN TA, use a standard serial cable to connect it to the Serial port on the Wireless Router.

6. Connect Printer Cable

Use a standard parallel printer cable to connect your printer to the Printer port on the Wireless Router.

7. Power Up

Connect the supplied power adapter and power up.
Use only the power adapter provided.

8. Check the LEDs

- The *Status* LED should flash, then turn Off. If it stays on, there is a hardware error.
- The *Power* LED should be ON.
- One (1) of the LAN LEDs (*10* or *100*) should be ON.
- The *Wireless* LED should be ON.
- If the printer is On and On-line, the *Print Act* LED should be ON.

For more information, refer to Top-mounted LEDs in Chapter 1.

Chapter 3
Configuration

This Chapter provides details of the configuration process.

Overview

This chapter describes the procedure for:

- Quick setup
- Wireless access point configuration
- Using the Status screens

PCs on your local LAN may also require configuration. For details, see *Chapter 4 - PC Configuration*.

Other configuration may also be required, depending on which features and functions of the Wireless Router you wish to use. Use the table below to locate detailed instructions for the required functions.

To Do this:	Refer to:
Configure PCs on your LAN.	Chapter 4: PC Configuration
Learn more about using DHCP on the internal LAN.	Chapter 5: DHCP
Configure and use the Serial (RS232) port, either for Internet access or for Dial-in.	Chapter 6: Serial Port
Configure various options: • Set a password for the Wireless Router, to protect the configuration data. • Disable NAT (Network Address Translation), • Enable TFTP firmware upgrade feature. • Configure Remote Management (configure via the Internet) • Access the Printer Port setup screen.	Chapter 7: Options
Configure the Wireless Router and other routers for a LAN which already has 1 or more routers.	Chapter 8: Routing
Use any of the following features: • Special Internet Applications • URL Filter • Virtual Servers • DMZ	Chapter 9: Advanced Internet Features
Limit Internet Access by individual workstations.	Chapter 10: Access Control

Where use of a certain feature requires that PCs or other LAN devices be configured, this is also explained in the relevant chapter.

Configuration Program

The Wireless Router contains an HTTP server. This enables you to connect to it, and configure it, using your Web Browser.

Most Browsers should work, provided they support HTML tables and forms.

Preparation

Before attempting to configure the Wireless Router, please ensure that:

- Your PC can establish a physical connection to the Wireless Router. The PC and the Wireless Router must be directly connected (using the "PC" port on the Wireless Router) or on the same LAN segment.
- The Wireless Router must be installed and powered ON.
- If the Wireless Router's default IP Address (192.168.0.1) is already used by another device, the other device must be turned OFF until the Wireless Router is allocated a new IP Address during configuration.

Connecting to the Wireless Router

To establish a connection from your PC to the device:

1. After installing the Wireless Router in your LAN, start your PC. If your PC is already running, restart it.
2. Start your WEB browser.
3. In the *Address* box, enter "HTTP://" and the IP Address of the Wireless Router, as in this example, which uses the Wireless Router's default IP Address:

   `HTTP://192.168.0.1`
4. You should then see the *Quick Setup* screen.
   See the following section for details on using this screen.

If you can't connect

If the Wireless Router does not respond, check the following:

- The Wireless Router is properly installed, LAN connection is OK, and it is powered ON.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- If your PC is using a fixed IP Address, its IP Address must be within the range 192.168.0.2 to 192.168.0.254 to be compatible with the Wireless Router's default IP Address of 192.168.0.1. Also, the *Network Mask* must be set to 255.255.255.0. See *Chapter 4 – PC Configuration* for details on checking your PC's TCP/IP settings.

Password

If you have assigned a password to the Wireless Router (on the *Options* screen) you will be prompted for the password, as shown below. (If no password has been set, this dialog will not appear.)

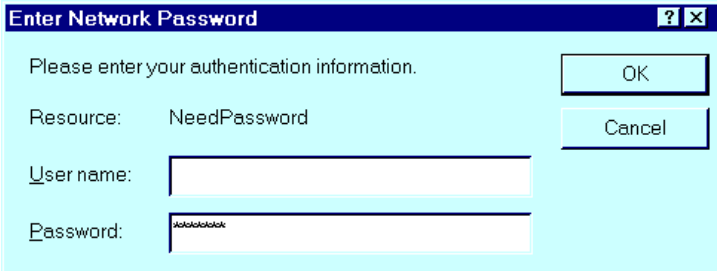


Figure 4: Password Dialog

- Leave the "User Name" blank.
- Enter the password for the Wireless Router, as set on the *Options* screen.

Navigation & Data Input

- Use the menu bar on the left of the screen, and the "Back" button on your Browser, for navigation.
- Changing to another screen without clicking "Save" does NOT save any changes you may have made. You must “Save” before changing screens or your data will be ignored.

On each screen, clicking this icon will display help for that screen.

Quick Setup Screen

The *Quick Setup* screen, like the example below, will be displayed when you first connect.

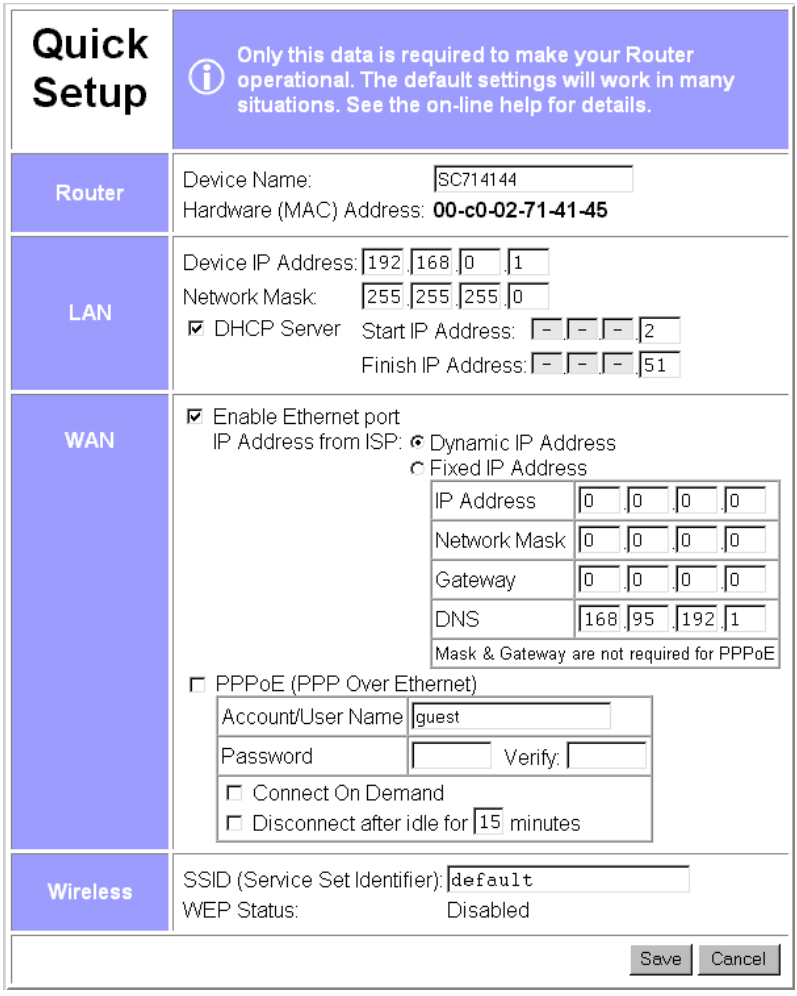

Quick Setup
Only this data is required to make your Router operational. The default settings will work in many situations. See the on-line help for details.
Router
Device Name: SC714144
Hardware (MAC) Address: 00-c0-02-71-41-45
LAN
Device IP Address: 192 .168 .0 .1
Network Mask: 255 .255 .255 .0
DHCP Server Start IP Address: - - - .2
Finish IP Address: - - - .51
WAN
Enable Ethernet port
IP Address from ISP: Dynamic IP Address
Fixed IP Address
IP Address 0 .0 .0 .0
Network Mask 0 .0 .0 .0
Gateway 0 .0 .0 .0
DNS 168 .95 .192 .1
Mask & Gateway are not required for PPPoE
PPPoE (PPP Over Ethernet)
Account/User Name guest
Password Verify:
Connect On Demand
Disconnect after idle for 15 minutes
Wireless
SSID (Service Set Identifier): default
WEP Status: Disabled
Save
Cancel

Figure 5: Quick Setup Screen

Quick Setup - Overview

This screen contains all the basic data to make the Wireless Router operational.

For many users, the default values will be satisfactory, and no changes will be required.

- **Router** Most users do not need to change these values.
- **LAN Settings** There is no need to change the LAN settings unless:
  - You wish to use a different IP Address range
  - You already have a DHCP Server or a Router on your LAN.
    See *Chapter 5 -DHCP* for more details about DHCP, or *Chapter 8 - Routing* for details about using Routers on your LAN.
- **WAN Port Settings** By default, the Wireless Router is configured for WAN access using a "Direct Connection" (cable modem or permanent DSL link) and a dynamic IP Address (the IP Address is supplied by your ISP when you connect). For this common situation, no changes are required.

- **Wireless Access Point** To use the Wireless Access Point:
  - All Wireless devices must have the same SSID. Either the Wireless Access Point or the Wireless clients can be changed to ensure this.
  - All Wireless devices must have the same settings for WEP (Wired Equivalent Privacy).
    By default, WEP on the Wireless Router is **Disabled**, so clients also need to have WEP **Disabled**.
  - See Appendix B for more details about Wireless LANs and WEP, and the *Wireless Screen* section later in this chapter for details of the Wireless Router's *Wireless* screen.

Configuration Data - Quick Setup Screen

Router	
Device (Host) Name	Normally, there is no need to change the default name, but if your ISP requests that you use a particular "Hostname", enter it here. This name will be provided to, and recorded by, the remote DHCP Server.
Hardware (MAC) Address	Also called *Network Adapter Address* or *Physical Address*. This is a low-level identifier for the Wireless Router, as seen from the WAN port. Provide this value to your ISP if requested. If you did not provide this value when first connected, there is no need to provide it now.
LAN	
Device IP Address	IP address for the Wireless Router, as seen from the local LAN. Use the default value of 192.168.0.1 unless the address is already in use or your LAN is using a different IP address range. In the latter case, enter an unused IP Address from within the range used by your LAN.
Network Mask	The default value 255.255.255.0 is standard for small (class "C") networks. For other networks, use the Network Mask for the LAN segment to which the Wireless Router is attached. i.e. the same value as the PCs on that LAN segment.
DHCP Server	See Chapter 5 for further details about DHCP. • If **Enabled**, the Wireless Router will allocate IP Addresses to PCs on your LAN. The default and recommended value is **Enabled**. • If you are already using a DHCP Server, this setting must be DISABLED, and the existing DHCP server must be re-configured as described in *Chapter 5 - DHCP*. • The **Start IP Address** and **Finish IP Address fields** set the values used by the DHCP server when allocating IP Addresses to DHCP clients. This range also determines the number of DHCP clients supported. (Maximum 253.)

WAN	
Enable Ethernet Port	Normally, this should be left at the default value of **Enabled**. • If no DSL or Cable modem is connected to the WAN (Ethernet) port, then this setting should be Disabled. • If Internet access via the Serial Port is Enabled, this setting will be automatically Disabled. It is not possible to simultaneously use both the WAN (Ethernet) port and the Serial (RS232) port for Internet access.
IP Address from ISP	**Dynamic IP Address**. This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Router upon connection. **Fixed IP Address**. Select this if your ISP has allocated you a fixed IP Address. If this option is selected, the following data must be entered. • **IP Address**. The IP Address allocated by the ISP. • **Network Mask (Not required for PPPoE)** This is also supplied by your ISP. It must be compatible with the IP Address above. • **Gateway IP Address (Not required for PPPoE)** The address of the router or gateway, as supplied by your ISP. • **DNS IP Address** The DNS (Domain Name Server) IP Address provided by your ISP. If required, additional DNS entries can be made on the *Options* screen.
PPPoE	If your ISP uses PPPoE, enable this checkbox and enter the data in the *PPPoE* section, as described below. If your ISP's data does not mention "PPPoE", do NOT enable this option.
Account/User Name	The "Login" name, or the name of the Internet account provided by your ISP.
Password and Verify	Enter the password for the above account. Re-enter the password in the *Verify* field, to ensure it is correct.
Connect on Demand	Normally, this should be Enabled. If disabled, you must use the *Connect* button on the ***Status*** screen to establish a connection.
Disconnect after Idle	Enable this if you wish an idle connection to be terminated. If enabled, enter the idle time-out period (in minutes) in the field provided. After the connection to your ISP has been idle for this time period, the connection will be terminated.
Wireless	
SSID (Service Set Identifier)	To communicate, all Wireless stations MUST use the same SSID/ESSID. You can either change this value, or change your client Wireless stations, to ensure this. The default SSID value for the Wireless Router is **`default`**. **Note! The SSID is case sensitive.**

WEP Status	This will state "Enabled" or "Disabled". The default is "Disabled". • In order to use the Wireless Router's access point, the client wireless stations must have the same settings for WEP. • To change the Wireless Router's WEP settings, use the ***Wireless*** screen, described in the following section.
Buttons	
Save	Save any data you have entered on this screen. Remember to save before changing to another screen.
Cancel	Cancel any changes you have made since the last "Save" operation.

Once this screen is completed, the Wireless Router is ready for use.

- If you wish to use WEP, or change other Wireless Access Point settings, refer to the following section.
- Your PCs may require configuration. Refer to *Chapter 4 - PC Configuration* for details.
- To check the status of the Wireless Router, and confirm that it is working correctly, refer to the *Status Screen* section later in this Chapter.

Wireless Screen

The Wireless Access Point settings must match the other Wireless stations. To change the Wireless Router's default settings for the Wireless Access Point, use the *Wireless* link on the main menu to reach the ***Wireless*** screen. An example screen is shown below.

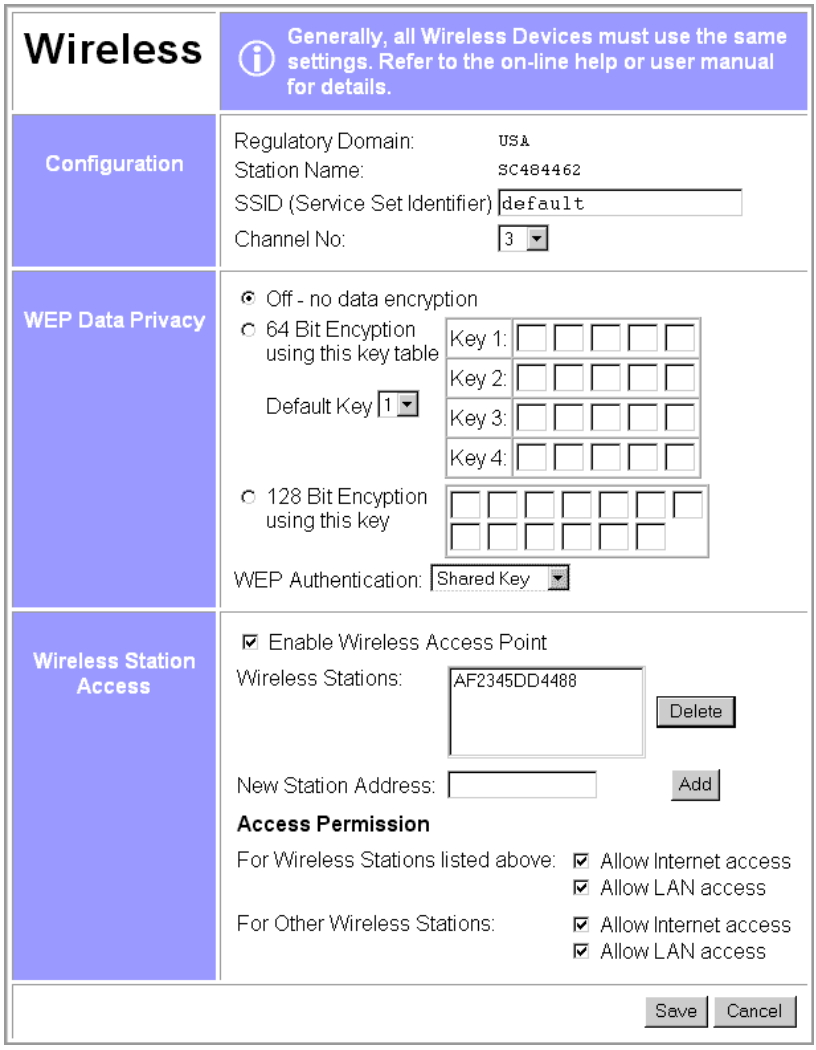


Figure 6: Wireless Screen

Data – Wireless Screen

Configuration	
Regulatory Domain	It is illegal to use this device in any location outside of the regulatory domain.
Station name	This is the same as the *Device (Host) Name* on the WAN screen. On your PC, some Wireless status screens may display this name as the Access Point in use.

SSID (ESSID)	To communicate, all Wireless stations MUST use the same SSID/ESSID. The default value is **`default`** **Note! The SSID is case sensitive.**
Channel No.	Select the value you wish to use on your Wireless LAN. If you experience lost connections and/or slow data transfers you may need to experiment with different channels to see which is the best.
WEP Data Privacy	
Off	If OFF (default), data is NOT encrypted before being transmitted.

64 Bit Encryption	• If selected, data is encrypted, using the default key, before being transmitted. The receiving station must be set to 64 Bit Encryption, and have the same Key value in the same position in its key table. Otherwise, it will not be able to decrypt the data.
	• **Default Key**
	Select the key you wish to be the default. Transmitted data is ALWAYS encrypted using the Default Key; the other Keys are for decryption only.
	• **Key Table**
	  • This table is used when Encrypting and Decrypting data. All stations, including this Access Point, always transmit data encrypted using their default key. The key number (1, 2, 3, 4) is also transmitted. The receiving station will use the key number (1, 2, 3, 4) to determine which key value to use for decryption. If the key value does not match the transmitting station, decryption will fail.
	  • The easiest way to ensure there are no problems is to have every Station, including the Access Point, use the same key table (all entries identical). Then, it does not matter which key is used as the default key.

128 Bit Encryption	• If selected, data is encrypted using the key before being transmitted. The receiving station must be set to use 128 Bit Encryption, and have the same Key value. Otherwise, it will not be able to decrypt the data. • **Key** Enter the key value you wish to use. Other stations must have the same key.
WEP Authentication	Select the appropriate value - "Open System" or "Shared Key". Check your Wireless card's documentation to see what method to use. Some Wireless cards do not support both methods.
Wireless Station Access	
Enable Wireless Access Point	• If enabled (default), this device can act as a Wireless Access Point. • If not enabled, no Wireless stations can use this device as a Wireless Access Point.

Existing Stations	• This lists the Wireless stations you have entered. If you have not entered any stations, this list will be empty. • To delete an entry, select it, and click the "Delete" button. Multiple entries may be selected by hold down the CTRL key while selecting. (On the Macintosh, use SHIFT instead of CTRL.)
New station Address	• Use this field to add a new station to the list. Just enter its address here, and click the "Add" button. • Use the software supplied with your Wireless unit to determine its address. The address consists of 12 letters (A..F) and digits (0..9) like this example: `10F810A81091` The address may be shown with separators (: or -) between each pair of characters. Do NOT enter the separators (: or -) in this field.
Access Permission	• **For Wireless Stations listed above** This setting determines what type of access is available to Wireless stations whose address has been entered in the "Wireless Stations" list. • **For Other Wireless Stations** This setting determines what type of access is available to Wireless stations whose address is NOT in the "Wireless Stations" list. • For either category, if neither "Internet" nor "LAN" access is enabled, Wireless stations are unable to use this Access Point.
Buttons	
Delete	**Delete** will delete the selected entry or entries in the list.
Add	**Add** will add the *New Station* data to the list.
Save	**Save** will save the other data on the screen. This has no effect on the contents of the ***Wireless Stations*** list.

Status Screen

Use the ***Status*** link on the main menu to view this screen.

The ***LAN Status*** link on the menu will result in a screen like the example below.

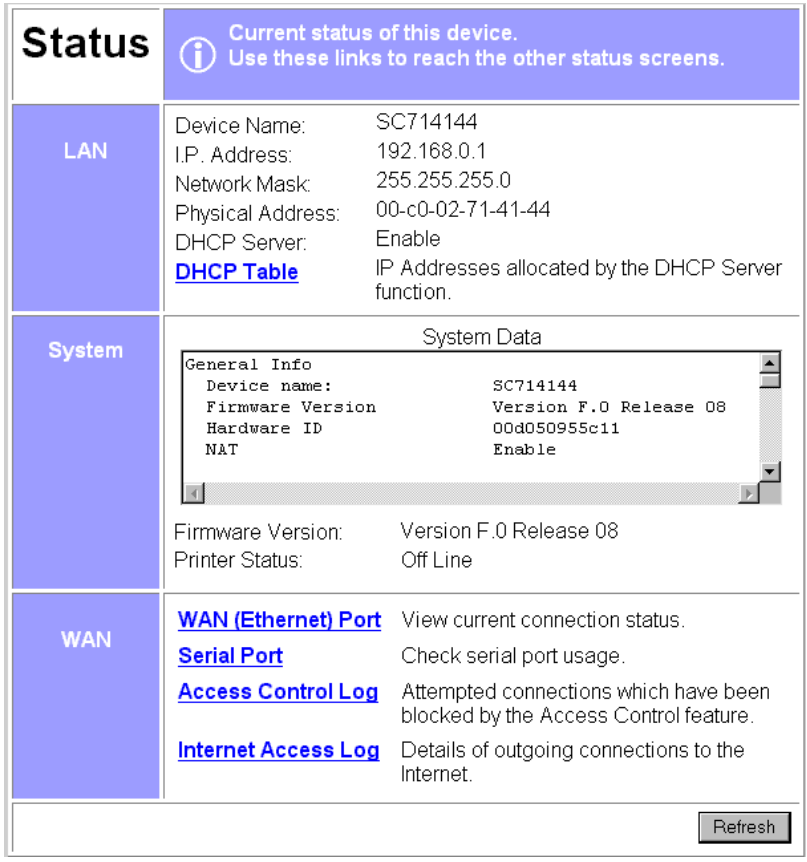


Figure 7: Status Screen

Data - Status Screen

LAN	
Device Name	This shows the name of the device.
IP Address	The IP Address of this device, as seen by other devices on the Internal LAN.
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
Physical Address	The "Hardware" address of this device, as seen by other devices on the Internal LAN.
DHCP Server	This shows the status of the DHCP Server function. The value will be "Enabled" or "Disabled".

DHCP Table	Use this link to view the IP Addresses which have been allocated to LAN devices, or the Dial-in user, by the DHCP Server function. The DHCP Table contains the following data: • **Port** - The port which the DHCP client used to access this device. Possible values are LAN, WLAN (Wireless LAN), and RS232 (serial port). • **IP Address** - The IP Address which has been allocated by the DHCP server to the DHCP client. • **Physical (Hardware) Address** - The Physical Address (Hardware Address) of the DHCP client which has been allocated this IP Address. • **Status** - Possible Status values are "Leased" (the IP Address is allocated to the device shown) or "Reserved" (the IP Address is reserved for this device, but not currently allocated). "Reserved" entries are generated for the Dial-in User, and for any PCs for which an IP Address has been reserved. An IP Address can be reserved for a particular PC using the *Access Control - PCs* screen. The *Access Control* feature is described in Chapter 10.
System	
System Data	This is identical to the data shown on a "Diagnostic Printout", and contains all system information.
Firmware Version	The version of the firmware currently installed in this device.
Printer Status	This shows the status of the printer. Click the "Refresh Screen" button to update this information.
WAN Links	
WAN (Ethernet) Port	View the WAN (Ethernet) status screen. This screen will vary according to the connection method used (Direct connection or PPPoE). See the following sections ***WAN Status - Direct Connection*** and ***WAN Status - PPPoE*** for details.
Serial Port	Check the status of the Serial Port. This screen is also accessible from the ***Serial Port*** sub-menu. See *Chapter 6 - Serial Port* for details of this screen.
Access Control Log	View details of connection attempts which have been blocked. See below for more information.
Internet Access Log	View details of outgoing connections to the internet. See below for more information.

Access Control Log

This log shows connection requests which have been blocked by the ***Access Control*** feature or the built-in NAT Firewall.

Accesses which have been blocked for other reasons (e.g. URL filter, incorrect dial-in password, incorrect WEP settings on the WLAN) are NOT shown in this log. (The "Internet Access Log" can be used to view connection attempts which have been blocked by the URL filter.)

Data shown in this log is as follows:

- **Port** - The port used to gain access to this device. Possible values are LAN, WAN, WLAN (Wireless LAN), and RS232 (serial port).
- **Source IP Address** - The IP Address of the PC or device whose access request was blocked.
- **Physical Address (Hardware Address)** - The hardware address of the PC or device whose access request was blocked.
- **Name** - If known, the name of the device whose access was blocked. This name is taken from the *Access Control* database. For Wireless devices, the name is obtained from the *Wireless Stations* list, and so will always match the Physical (Hardware) address.
- **Destination** - The destination of the attempted access. Possible values are "Internet", "LAN" or "WLAN".
  - "Internet" indicates an attempt by a LAN user, WLAN user, or dial-in user to access the Internet using a protocol and/or port number which was blocked.
  - "LAN" or "WLAN" indicates a connection attempt from the Internet which was not allowed. The protocol (TCP or UDP) and port number are shown in braces.

    This data is useful if you want the access to be allowed. In this case, you can use this data to configure the *Advanced Internet - User-defined Virtual Servers* screen or the *Advanced Internet - Special Applications* screen. (In the case of a Special Application, this log indicates the "Incoming Connection" for the Special Application.)

    See *Chapter 9 - Advanced Internet* for further details of the *Virtual Server* and *Special Applications* features.

Internet Access Log

This log shows details of Internet access by LAN users, WLAN users, or the dial-in user.

Details shown in this log are as follows:

- **Source IP Address** - The IP Address of the LAN user, WLAN user, or dial-in user making the connection request.
- **Destination** - The requested Internet IP Address or URL. Normally, the IP Address will be shown. But if the *URL Filter* feature is Enabled, the URL will be displayed.
  For details on using the *URL Filter*, refer to *Chapter 9 - Advanced Internet*.
- **Blocked** - This will indicate "Yes" if the connection attempt was blocked by the URL Filter. Otherwise, this will be blank.

WAN Status – Direct Connection

If the WAN (Ethernet) port is using PPPoE, then clicking the *WAN Status* link on the *Status* screen will reveal a screen like the following.

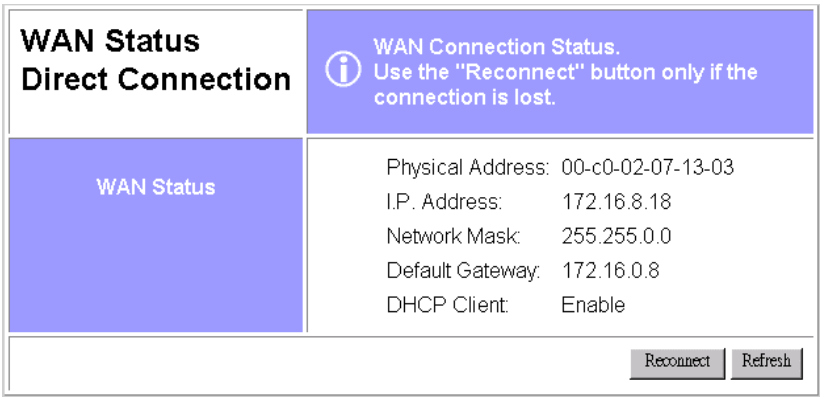


Figure 8: WAN Status – Direct Connection

Data

WAN Status	
Physical Address	The "Hardware" address of this device, as seen by other devices on the WAN.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask for the above IP Address.
Default Gateway	IP address of the Router/Gateway on the WAN port.
DHCP Client	Displays "Enabled" or "Disabled", indicating whether this device is acting as a DHCP client on the external LAN or WAN.
Buttons	
Reconnect	Use this button if the connection seems to have been lost, and no data is being transferred. (This button has no effect unless acting as a DHCP Client.)
Refresh	Update the data on screen.

WAN Status – PPPoE

If the WAN (Ethernet) port is using PPPoE, then clicking the *WAN Status* link on the *Status* screen will reveal a screen like the following.

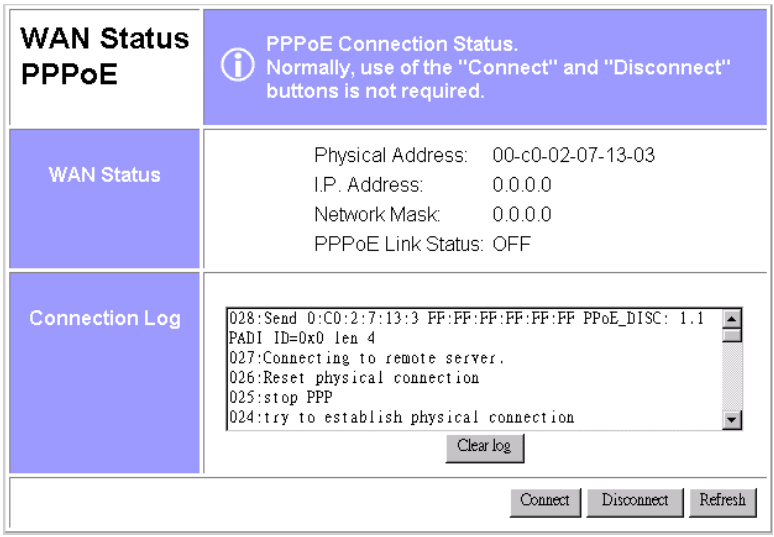


Figure 9: WAN Status – PPPoE

Status Data

WAN Status	
Physical Address	The "Hardware" address of this device, as seen by other devices on the WAN.
IP Address	The IP Address of this device, as seen by devices on the WAN. (This device has 2 IP Addresses; one for the local LAN, and another for the WAN port.)
Network Mask	The Network Mask (Subnet Mask) for the IP Address above.
PPPoE Link Status	This indicates whether or not the connection is currently established. If the connection does not exist, the ***Connect*** button can be used to establish a connection. If the connection currently exists, the ***Disconnect*** button can be used to break the connection.
Connection Log	
Log Data	This shows status messages relating to the existing connection. The most common messages are listed in the following table.
Buttons	
Connect	If not connected, establish a connection to your ISP
Disconnect	If connected to your ISP, hang up the connection.
Clear Log	Delete all data currently in the Log. This will make it easier to read new messages.
Refresh	Contact this device and update the Log data.

Connection Log Messages

Message	Description
Connect on Demand	Connection attempt has been triggered by the "Connect on Demand" setting.
Manual connection	Connection attempt started by the "Connect" button.
Reset physical connection	Preparing line for connection attempt.
Connecting to remote server	Attempting to connect to the ISP's server.
Remote Server located	ISP's Server has responded to connection attempt.
Start PPP	Attempting to login to ISP's Server and establish a PPP connection.
PPP up successfully	Able to login to ISP's Server and establish a PPP connection.
Idle time-out reached	The connection has been idle for the time period specified in the "Idle Time-out" field. The connection will now be terminated.
Disconnecting	The current connection is being terminated, due to either the "Idle Time-out" above, or "Disconnect" button being clicked.
Error: Remote Server not found	ISP's Server did not respond. This could be a Server problem, or a problem with the link to the Server.
Error: PPP Connection failed	Unable to establish a PPP connection with the ISP's Server. This could be a login problem (name or password) or a Server problem.
Error: Connection to Server lost	The existing connection has been lost. This could be caused by a power failure, a link failure, or Server failure.
Error: Invalid or unknown packet type	The data received from the ISP's Server could not be processed. This could be caused by data corruption (from a bad link), or the Server using a protocol which is not supported by this device.

Chapter 4
PC Configuration

This Chapter details the PC Configuration required on the local ("Internal") LAN.

Overview

For each PC, the following may to be configured:

- TCP/IP network settings
- Internet Access configuration
- Network printer
- Wireless configuration

Windows Clients

This section describes how to configure Windows clients for:

- Internet access via the Wireless Router
- Printing using the printer attached to the Wireless Router.
- Remote Dial-in access to the modem attached to the Wireless Router's serial (RS232) port.

The first step is to check the PC's TCP/IP settings.

The Wireless Router uses the TCP/IP network protocol for all functions, so it is essential that the TCP/IP protocol be installed and configured on each PC.

TCP/IP Settings

If using the default Wireless Router settings, and the default Windows 95/98 TCP/IP settings, no changes need to be made.

- By default, the Wireless Router will act as a DHCP Server, automatically providing a suitable IP Address to each PC when the PC boots.
- The default Windows 95/98 TCP/IP setting is to act as a DHCP client.

To check your PC's TCP/IP Settings:

1. Select *Control Panel - Network*. You should see a screen like the following:

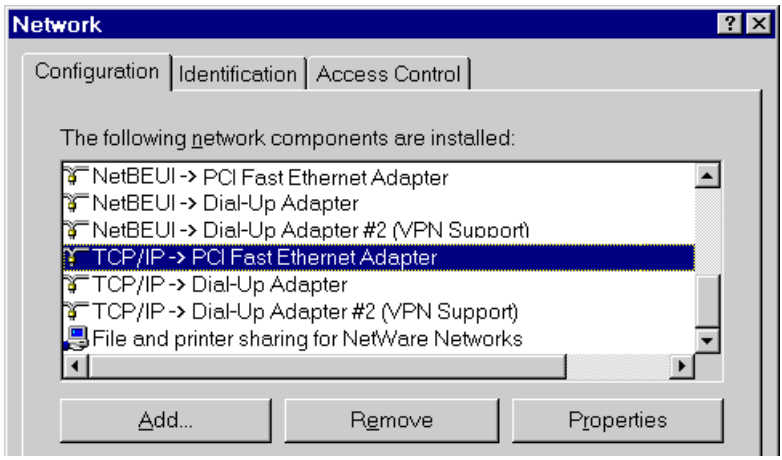


Figure 10: Network Configuration

2. Select the *TCP/IP* protocol for your network card.
3. Click on the *Properties* button. You should then see a screen like the following.

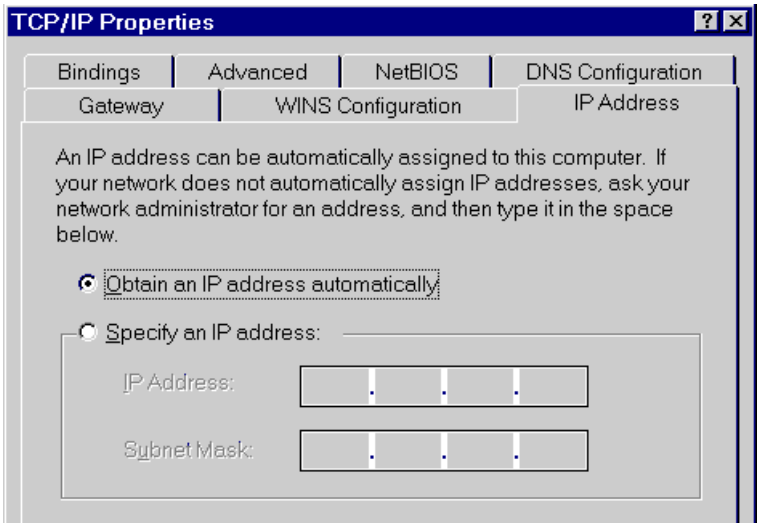

TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:

Figure 11: IP Address (Win 95)

Ensure your TCP/IP settings are correct, as follows:

Using DHCP

To use DHCP, select the radio button *Obtain an IP Address automatically*. This is the default Windows settings.

Restart your PC to ensure it obtains an IP Address from the Wireless Router.

Using "Specify an IP Address"

- If your PC is already configured, do NOT change the settings on the IP Address tab shown in Figure 11 above.
- On the *Gateway* tab, enter the Wireless Router's IP address in the *New Gateway* field and click *Add*. Your LAN administrator can advise you of the IP Address they assigned to the Wireless Router.

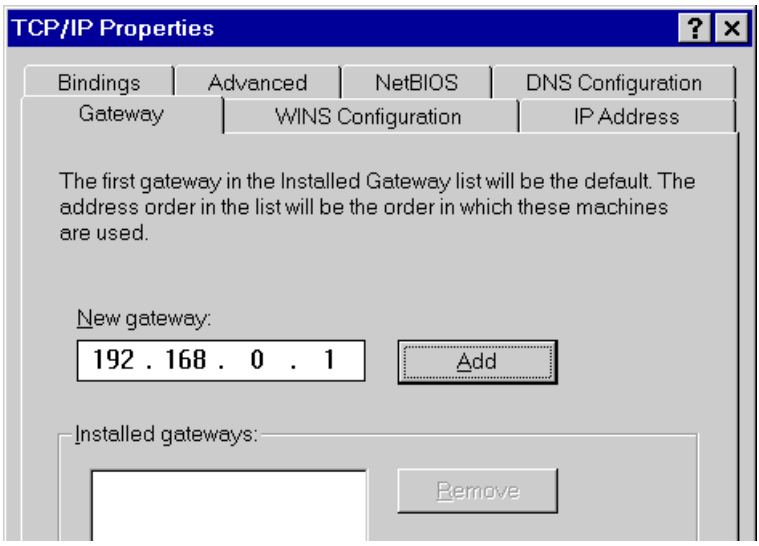


Figure 12: Gateway Tab (Win 95/98)

- On the *DNS Configuration* tab, ensure *Enable DNS* is selected. If the *DNS Server Search Order* list is empty, enter the DNS address provided by your ISP in the fields beside the *Add* button, then click *Add*.

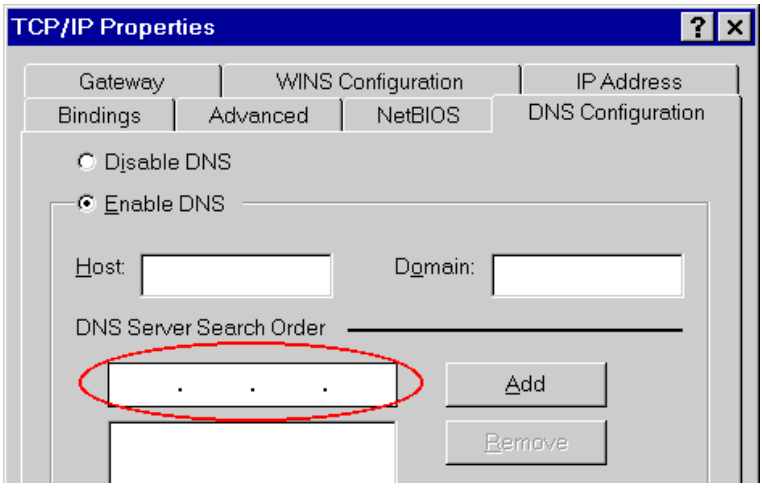


Figure 13: DNS Tab (Win 95/98)

If your LAN has a Router, the LAN Administrator must re-configure the Router itself. Refer to *Chapter 8 - Routing* for details.

Internet Access

If you are using the Wireless Router for Internet access:

- Ensure that the DSL modem, Cable modem, or other permanent connection is functional.
- Use the following procedure to configure your Browser to access the Internet via the LAN, rather than by a Dial-up connection.

1. Select *Start Menu - Settings - Control Panel - Internet Options*.
2. Select the *Connection* tab, and click the *Setup* button.
3. Select "I want to set up my Internet connection manually, or I want to connect through a local area network (LAN)" and click "Next".
4. Select "I connect through a local area network (LAN)" and click "Next".
5. Ensure all of the boxes on the following *Local area network Internet Configuration* screen are **unchecked**.
6. Check the "No" option when prompted “Do you want to set up an Internet mail account now?”.
7. Click "Finish" to close the Internet Connection Wizard.
8. Then simply use your Browser, FTP client, or other Internet client to connect to the desired Internet site.

Accessing AOL

To access AOL (America On Line) through the Wireless Router, the *AOL for Windows* software must be configured to use TCP/IP network access, rather than a dial-up connection. The configuration process is as follows:

- Start the *AOL for Windows* communication software. Ensure that it is Version 2.5, 3.0 or later. This procedure will not work with earlier versions.
- Click the *Setup* button.
- Select *Create Location*, and change the location name from "New Locality" to "Wireless Router".
- Click *Edit Location*. Select *TCP/IP* for the *Network* field. (Leave the *Phone Number* blank.)
- Click *Save*, then *OK*.
  Configuration is now complete.
- Before clicking "Sign On", always ensure that you are using the "Wireless Router" location.

Printing Setup

The Wireless Router provides printing support for 2 methods of printing from Windows:

- **Print Port Driver.** After installing the Print Port Driver, Windows users can print directly to the Wireless Router. Print jobs are spooled (queued) on each PC.
  The supplied Print Port Driver supports Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.
- **LPD/LPR Printing.** If using Windows NT 4.0 Server or Windows 2000 Server, LPD/LPR printing can be used. No software needs to be installed on either the Windows Server or each client PC. Print jobs will be spooled (queued) on the Windows Server, and can be managed using the standard Windows Server tools.

Print Port Driver Setup

The following procedure is for Windows 95/98, Windows ME, Windows NT4.0, and Windows 2000.

1. Insert the supplied CD-ROM into your drive. If the setup program does not start automatically, run SETUP.EXE in the root folder.
2. At the *Setup Type* screen, select the correct model.
3. At the *Select Components* screen, select the ***Print Port Driver*** option.
4. Follow the prompts to complete the installation.
5. The *Print Port Setup* will then run, and the following screen will be displayed.

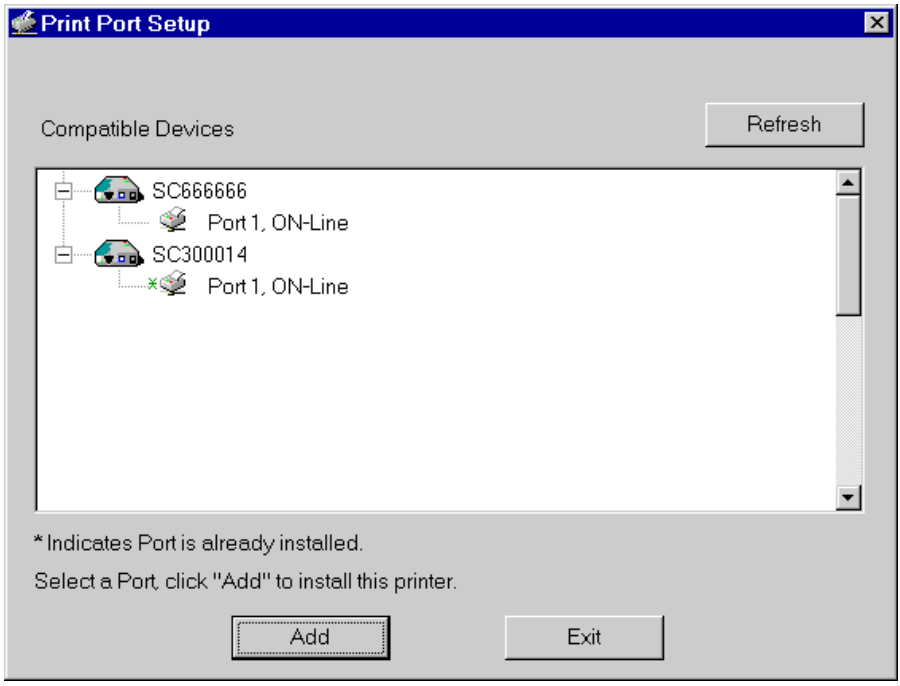
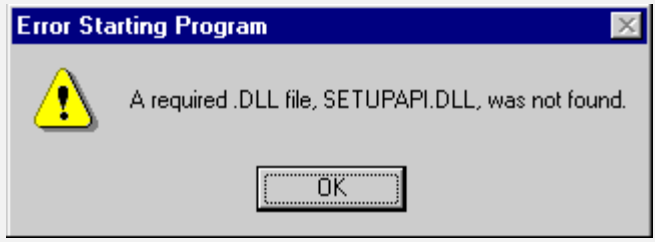


Figure 14: Print Port Setup

6. Select the desired device and port, and then click the "Add" button.

If you see the following error message, either install Internet Explorer 4 or later, or follow the procedure in the "Trouble Shooting - Printing" section of Appendix A.



7. A pop-up message will inform you if the port has been created successfully, and then the Windows *Add Printer* wizard will start.
   - Select the correct Printer Manufacturer and Model, or use the "Have Disk" option if appropriate.
   - If desired, change the Printer name so it indicates the device used (e.g. HP2100 on SCA43600)
   - If prompted about Sharing, do NOT enable Sharing.
8. Installation is now complete. You can now print using this printer.
   - To install additional Printers, repeat steps 6 and 7.
   - Use the ***Start*** menu to run this program in future. The default installation is *Start - Programs - Broadband Internet Router - Add Port*.

Management

- Print jobs can be managed like any Windows printer. Open the *Printers* folder (*Start - Settings - Printers*) and double-click any printer to see the current print jobs.
- If the printer attached to the Wireless Router is changed, just run this program again, and select the correct printer.
- To delete a port created by this setup program, use the Windows *Delete Port* facility:
  - Right-click any printer in the *Printers* folder, and select *Properties*.
  - Locate the *Delete Port* button. This button is on the *Details* or *Ports* tab, depending on your version or Windows.
- If the Wireless Router's IP Address is changed, and you can no longer print, delete the port (see procedure above) and re-install it.

Port Options

The options for the *Print Port Driver* are accessed via the Windows *Port Settings* button.

Use *Start - Settings - Printers* to open the Printers folder, then right-click the Printer, and select *Properties*. The *Port Settings* button is on the *Details* or *Port* tab, depending on your version of Windows.

An example screen is shown below:

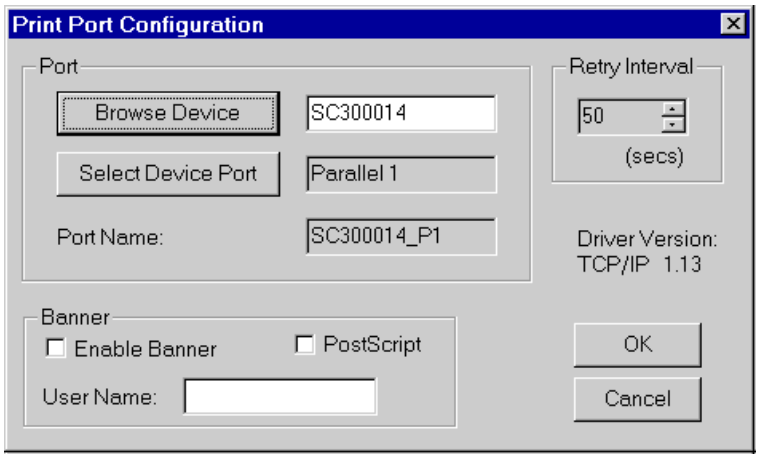


Figure 15: Print Port Configuration

Items shown on this screen are as follows:

Port	If desired, click *Browse* to select a different device. (The *Select Device Port* button is provided to allow this software to work with multi-port models.) The *Port Name* is shown in the Printer's *Properties*.
Banner	Check this option to print a banner page before each print job. • If using a PostScript Printer, check the *PostScript* box. • The *User Name* will be printed on the banner page.
Retry Interval	Sets how often Windows will poll the Wireless Router to establish a connection when the printer is busy. Increase this value if you get too many warning messages.

LPD/LPR Printing

LPD/LPR printing can be used with Windows NT 4.0 Server or Windows 2000. No software needs to be installed.

Windows NT 4.0 Server Configuration

To use LPD printing, **Microsoft TCP/IP Printing** must be installed and enabled. This can be checked using *Start-Settings-Control Panel-Network - Services*.

To install LPD printing using the Wireless Router, follow this procedure:

1. Go to *Start-Settings-Printer* and invoke the *Add Printer* wizard.
2. When prompted with "This printer will be managed by..", select **My Computer** and click Next.
3. Select **Add Port…**, then select **LPR Port** and click **New Port**.
4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the Wireless Router.
5. For *Name of printer or print queue on that server*, enter L1
6. Click OK. When returned to the Printer Ports window, simply select *Close* and then install your printer driver as usual.
7. When prompted whether or not the printer will be shared, select the **Sharing** radio button.

8. In the *Shared* dialog box, enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
9. Click OK to save and exit.

Windows 2000 Server Configuration

The *LPD/LPR Port* is not enabled by default. To enable it, use this procedure:

1. In *Control Panel*, select *Add/Remove Programs*, then *Windows Components*.
2. Select *Other Network File and Print Services*, then click the *Details* button.

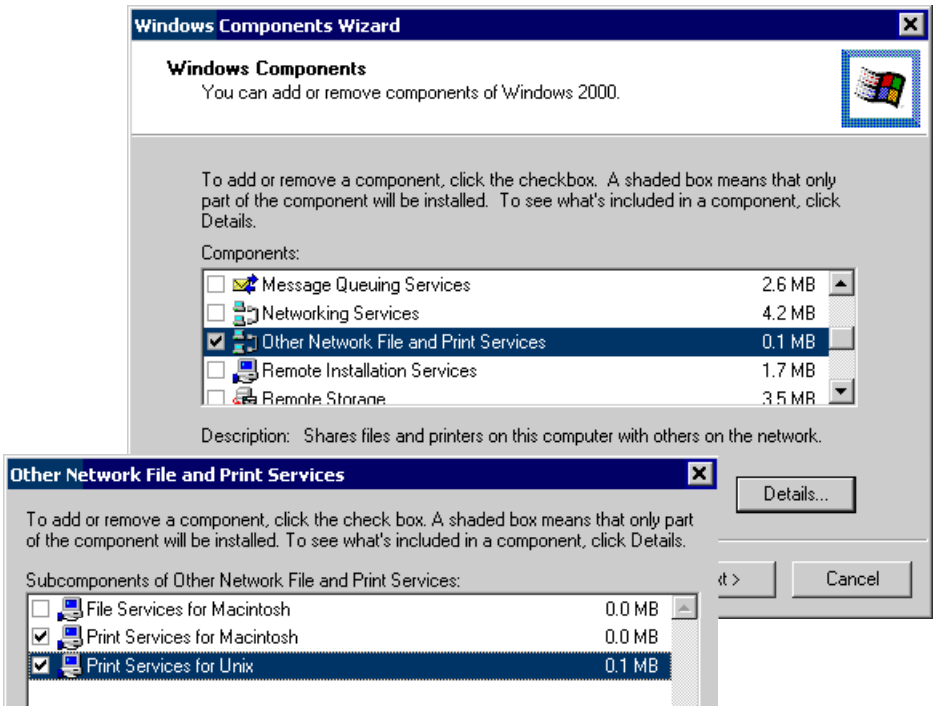

Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Message Queuing Services 2.6 MB
Networking Services 4.2 MB
Other Network File and Print Services 0.1 MB
Remote Installation Services 1.7 MB
Remote Storage 3.5 MB
Description: Shares files and printers on this computer with others on the network.
Details...
Other Network File and Print Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Other Network File and Print Services:
File Services for Macintosh 0.0 MB
Print Services for Macintosh 0.0 MB
Print Services for Unix 0.1 MB
Cancel

Figure 16: Adding LPD/LPR Port (Win 2000)

3. Enable *Print Services for Unix*, and click OK.
4. Click *Next* and complete the Wizard.

Adding the Printer

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Local Printer*.
3. On the *Select the Printer Port* screen, select *LPR Port*, as shown below. Click *Next* to continue.

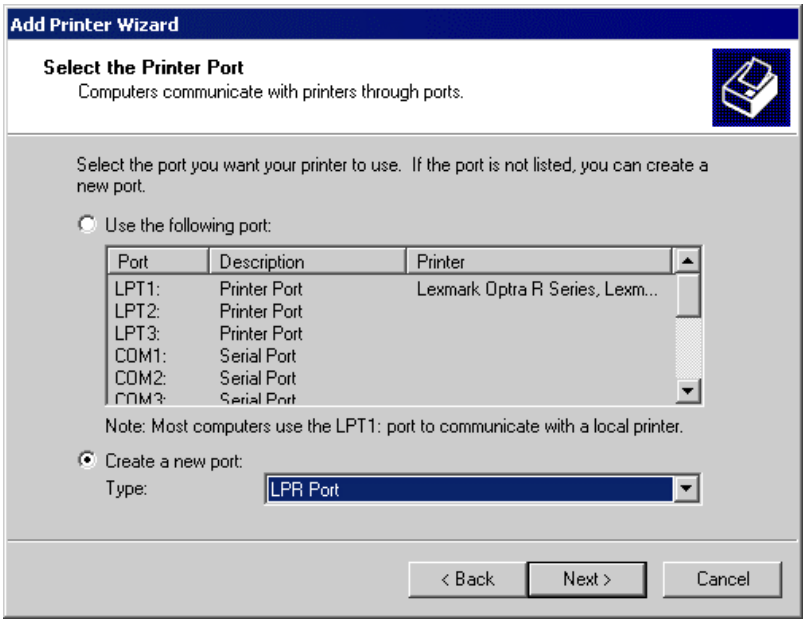


Figure 17: Windows 2000: Select Port

4. In the Dialog requesting *Name of Address of server providing lpd*, enter the IP address of the Wireless Router.
5. For *Name of printer or print queue on that server*, enter L1.
6. Click OK, and then *Next*, and continue the Wizard.
7. At the *Select Sharing* screen, select the Radio Button for *Share As*, and enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
8. Complete the *Add Printer* wizard.

Client PC Setup for LPD/LPR Printing

After configuring the Windows Server, client PCs on the LAN can install the new printer.

The following procedure is for Windows 95/98/ME, Windows NT4.0, and Windows 2000 workstation.

1. Open your *Printers* folder, and start the *Add Printer* Wizard.
2. When prompted, select *Network Printer*.
3. When prompted for *Network Path or Queue Name*, click the *Browse* button, and locate the Server and Printer which your Network Administrator advised you to use.
4. Click OK, then *Next*.
5. Select the correct printer Manufacturer and Model, as advised by your Network Administrator, and click *Next*.
6. Follow the prompts to complete the Wizard.
7. The new printer will be listed with any other installed printers, and may be selected when printing from any Windows application.

Dial-in Configuration

This section describes how to configure your PC to use the Wireless Router's RAS Dial-in feature.

To use the RAS Dial-in feature of the Wireless Router:

- An Analog Modem or ISDN TA must be connected to the Serial Port on the Wireless Router.
- The Wireless Router's ***Serial Port*** screen must be configured for Dial-in access, and Dial-in Users must be created. See *Chapter 6 - Serial Port* for details.
- A suitable Dial-up connection must be created on your PC, as described below.

Creating a Dial-in Connection in Windows

You can use the standard Windows *Dial-up Networking* software normally used for Internet access. The procedure is as follows:

1. Ensure your modem is installed and working.
2. Select *My Computer*, then *Dial-up Networking*.
3. Click *Make new Connection*, and step through the Wizard.
   - Give this connection a suitable name.
   - Enter the area code and telephone number to connect to the Wireless Router.
   - Continue the Wizard until completed.
4. The default values for this connection will work with the Wireless Router's default values. If necessary, you can adjust the *Properties* for the connection:
   - In the *Dial-up Networking* window, select the connection.
   - Right-click, and select *Properties* to see a screen like the one below.

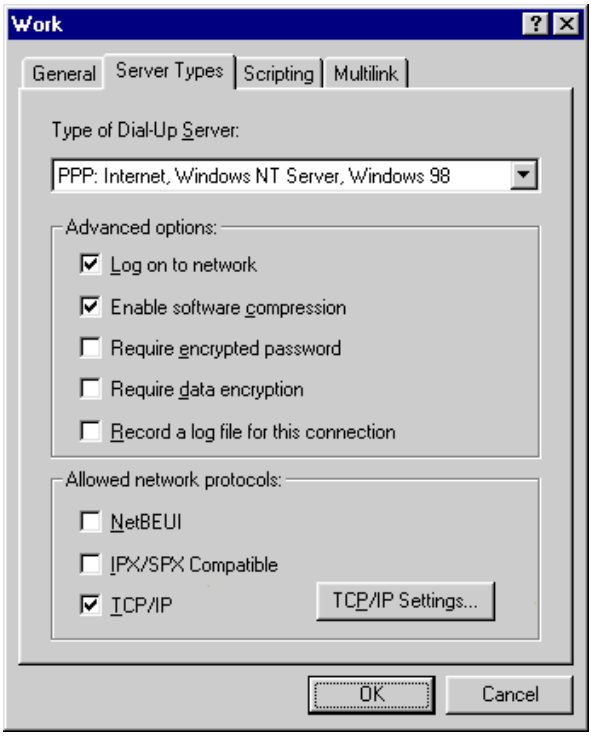


Figure 18: Dial-up Networking Properties

Dial-up Networking Properties

Log on to network	This setting refers to a logon to a Server on your LAN, not the login to the Wireless Router. This is checked by default, but to work correctly, your PC needs to be configured with a valid network logon (in your PCs network properties). If no network logon is defined, checking this option will cause a minor delay in establishing a connection.
Enable software compression	Normally, this should be checked, but the Wireless Router will function with either Checked or Unchecked.
Required encrypted password	The **Unchecked** state corresponds to the "PAP" setting on the Wireless Router's *Serial Port* screen. The **Checked** setting corresponds to the "MSCHAP" setting on the Wireless Router's *Serial Port* screen.
Require data encryption	This must NOT be checked.
Network Protocols	NetBEUI and IPX/SPX can be disabled.
TCP/IP Settings	The default settings should not be changed.

Using the Dial-in Connection

1. In the *Dial-up Networking* window, double-click the connection to start the dial-in process.
2. When prompted for a user name and password, enter the Name and Password assigned to you (this is done on the Wireless Router's *User Details* screen).
3. If the Wireless Router's *Callback* feature is enabled, the connection will then be terminated, and your modem must wait for the incoming call from the Wireless Router's modem.
4. Upon connection, the Wireless Router will allocate an IP Address to your PC. To other LAN users and devices, you will appear to be a normal LAN user.
5. If you have defined a network logon using a Server on the remote LAN, and the *Log on to network option* in *Figure 18: Dial-up Networking Properties* is checked, then you will be prompted for your network logon.

Macintosh Clients

Internet Access

From your Macintosh, you can access the Internet via the Wireless Router. The procedure is as follows.

1. Open the TCP/IP Control Panel.
2. Select *Ethernet* from the *Connect via* pop-up menu.
3. Select *Using DHCP Server* from the *Configure* pop-up menu. The DHCP Client ID field can be left blank.
4. Close the TCP/IP panel, saving your settings.

Note:

If using manually assigned IP addresses instead of DHCP, the only change required is to set the *Router Address* field to the Wireless Router's IP Address.

Printing

If you wish to share the printer connected to the Wireless Router, using a LaserWriter or compatible is strongly recommended.

If the printer connected to the Wireless Router is NOT a LaserWriter, ensure that:

- The *Printer Object Type* on the Wireless Router's *Printer Port* screen is set correctly.
- Each Macintosh has the correct printer driver for the printer. The Wireless Router will not process the print data in any way, but merely forward it to the printer.

Installing the Printer

To gain access to the printer connected to the Wireless Router, follow this procedure:

1. Select *Control Panel - Network*.
2. Ensure that *EtherTalk* is selected under *AppleTalk Connection*.
3. Open *Chooser*, and select the correct printer type (e.g. LaserWriter).
4. From the list of available printers on the right, select the Wireless Router, then click *Create*.
5. The new printer will be created, and can be used like any other printer.

Linux Clients

Internet Access on Linux

Ensure you are logged in as "root" before attempting any changes.

By default, most Unix installations use a fixed IP Address. If you wish to continue using a fixed IP Address, make the following changes to your configuration.

- Set your "Default Gateway" to the IP Address of the Wireless Router.
- Ensure your DNS (Nameserver) settings are correct.

To act as a DHCP Client (recommended)

The procedure below may vary according to your version of Linux and X -windows shell.

1. Start your X Windows client.
2. Select *Control Panel - Network*
3. Select the "Interface" entry for your Network card. Normally, this will be called "eth0".
4. Click the *Edit* button, set the "protocol" to "DHCP", and save this data.
5. To apply your changes
   - Use the "Deactivate" and "Activate" buttons, if available.
   - OR, restart your system.

LPD Printing on Linux

The procedure below may vary according to your version of Linux and X -windows shell.

1. In your X Windows shell, select *Control Panel*, then *Printer Configuration*.
2. Select *Add*. For the printer type, select *Remote Unix (lpd) Queue*.
3. Use the following data to complete the resulting dialog.

Field	Data	Example
Name	Enter a name for this printer	gw_prn
Spool Directory	/var/spool/lpd/*printer_name* Where *printer_name* is the "Name" entry above.	/var/spool/lpd/gw_prn
File Limit	Enter a suitable number.	0 (no limit)
Remote Host	Wireless Router's IP address	192.168.0.1
	Note: If you have made a host file entry, you can use the name from the host file instead of the IP Address.	
Remote Queue	L*n* Where *n* is the Logical Printer number (L1, L2, L3). Logical Printers can be configured on the Wireless Router's *Options- Printer Port* screen.	L1

4. Save this data, and exit the Printer Configuration. Configuration is now completed, and the printer is now available for use.

Other Unix Systems

For Internet Access via the Wireless Router

- Ensure the "Gateway" field for your network card is set to the IP Address of the Wireless Router.
- Ensure your DNS settings are correct.

LPD Printing

To use LPD printing to the Wireless Router's printer, install an LPD printer using the standard procedure for your system.

- Use the Wireless Router's IP Address as the location of the remote host
- Use L1, L2, or L3 for the name of the printer on the remote host.

On the Wireless Router, the logical printers (L1, L2, and L3) can be configured on the *Options - Printer Port* screen.

Wireless Station Configuration

This section applies to all Wireless stations wishing to use the Wireless Router's Access Point, regardless of the operating system which is used on the client.

To use the Wireless Access Point in the Wireless Router, each Wireless Station must have compatible settings, as follows:

Mode	The mode must be set to ***Infrastructure***.
SSID (ESSID)	This must match the value used on the Wireless Router. The default value is **`default`** **Note! The SSID is case sensitive.**
WEP	By default, WEP on the Wireless Router is **disabled**. • If WEP remains disabled on the Wireless Router, all stations must have WEP disabled. • If WEP is enabled on the Wireless Router, each station must use the same settings as the Wireless Router.

Chapter 5
DHCP

This Chapter covers the use of DHCP, using either an existing DHCP Server or the Wireless Router's DHCP Server function.

Overview

If your LAN does not use DHCP, and you do not wish to use DHCP, you can ignore this chapter.

What DHCP Does

A DHCP (Dynamic Host Configuration Protocol) **server** allocates a valid IP address to a DHCP **client** (PC or device) upon request.

- The client request is made when the client device boots.
- The DHCP Server provides the *Gateway* and *DNS* addresses to the client, as well as allocating an IP Address.
- Windows 95/98/ME include all the software required to act as a DHCP **client**. This is the default Windows setting for TCP/IP. However, Windows uses the term *Obtain an IP Address automatically* instead of "DHCP Client".
- The Wireless Router can act as a **DHCP server**.

Using the Wireless Router's DHCP Server

This is the default setting. The DHCP Server settings are on the ***LAN*** screen. On this screen, you can:

- Enable or Disable the Wireless Router's *DHCP Server* function.
- Set the range of IP Addresses allocated to PCs by the DHCP Server function.

You can assign Fixed IP Addresses to some devices while using DHCP, provided that the Fixed IP Addresses are NOT within the range used by the DHCP Server.

Using another DHCP Server

You can only use one (1) DHCP Server. If you wish to use another DHCP Server, rather than the Wireless Router's, the following procedure is required.

1. Disable the DHCP Server feature in the Wireless Router. This setting is on the LAN screen.
2. Configure the DHCP Server to provide the Wireless Router's IP Address as the *Default Gateway*.

To Configure your PCs to use DHCP

This is the default setting for TCP/IP under Windows 95/98/ME. See *Chapter 4 – Client Configuration* for the procedure to check these settings.

Chapter 6
Serial Port

6

This Chapter details using the Serial (RS232) Port, either for Internet Access or Dial-in use.

Overview

The Serial (RS232) port can be used for Internet Access or to provide RAS (Dial-in) access to your LAN.

- If used for Internet access, the WAN (Ethernet) Port cannot be used.
- Both *Internet Access* and *Dial-in Access* can be enabled simultaneously, but if the modem is in use, a Dial-in user will only get a "busy" signal on their telephone line.

Serial Port Screen

This screen is reached via the *Serial Port* link on the main menu.

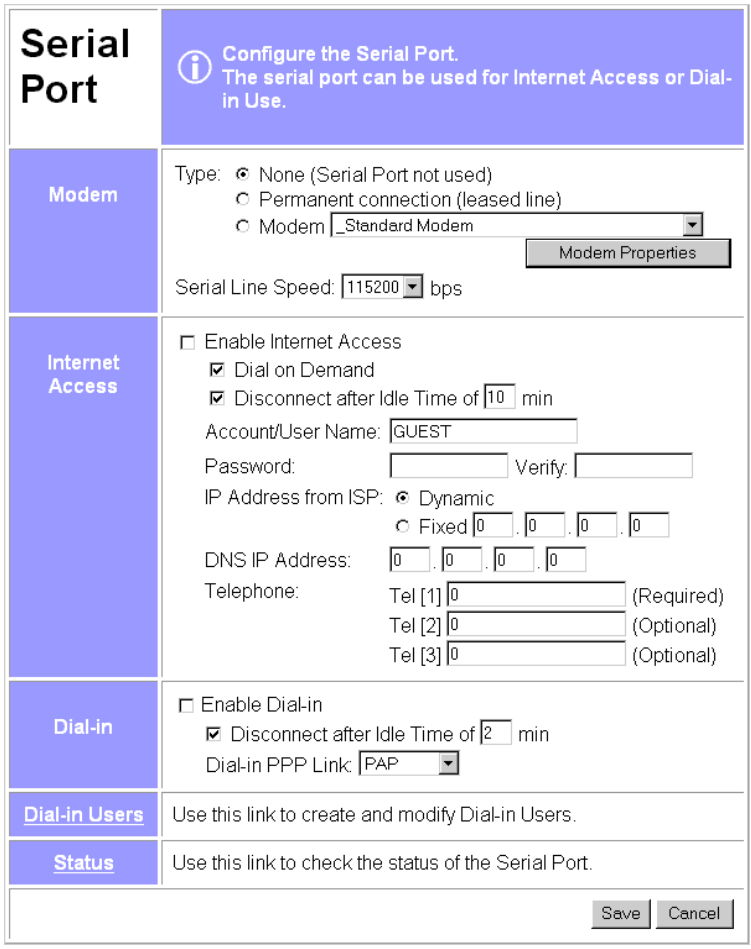

Serial Port
Configure the Serial Port.
The serial port can be used for Internet Access or Dial-in Use.
Modem
Type: None (Serial Port not used)
Permanent connection (leased line)
Modem _Standard Modem
Modem Properties
Serial Line Speed: 115200 bps
Internet Access
Enable Internet Access
Dial on Demand
Disconnect after Idle Time of 10 min
Account/User Name: GUEST
Password: Verify:
IP Address from ISP: Dynamic
Fixed 0 . 0 . 0 . 0
DNS IP Address: 0 . 0 . 0 . 0
Telephone:
Tel [1] 0 (Required)
Tel [2] 0 (Optional)
Tel [3] 0 (Optional)
Dial-in
Enable Dial-in
Disconnect after Idle Time of 2 min
Dial-in PPP Link: PAP
Dial-in Users
Use this link to create and modify Dial-in Users.
Status
Use this link to check the status of the Serial Port.
Save
Cancel

Figure 19: Serial Port Screen

Data - Serial Port Screen

Modem	
Type	Select ***None*** if nothing is connected to the Serial Port, or you do not wish use to use the Serial Port. For ***Permanent Connection (leased line)*:** • Ensure the *Serial Line Speed* is set to match the speed on your leased line. • Ignore the Telephone numbers and "Disconnect after Idle" setting. For ***Modem***: • If your modem is in the drop-down list, just select it. • If your modem is not in the list, select "_Standard Modem" and test to see if this works. • If "_Standard Modem" does not work, select "Other", then click the *Modem Properties* button and set these settings correctly. See the section *Modem Properties Screen* later in this chapter for further details.
Modem Properties	Clicking this button will open the ***Modem Properties*** screen and allow changing of the modem's properties. Normally, this is not required. See the section *Modem Properties Screen* later in this chapter for further details.
Serial Line Speed	Select the speed which is equal to or below the fastest **Serial** line speed (NOT Phone line speed) of your modem. Available speeds range from 4.8K to 460.8K (bps).
Internet Access	
Enable Internet Access	Use this to enable or disable Internet access on this port. **Checking this box will disable Internet Access via the WAN (Ethernet) port, because both methods cannot be used simultaneously.** However, for the Serial Port, both Dial-in and Internet can be enabled simultaneously.
Dial on Demand	If checked, an Internet connection will be established automatically, whenever required. If not checked, the Internet connection must be established manually, using the *Dial-up* button on the *Serial Port Status* screen.
Disconnect after Idle Time	If checked, an Internet connection will be terminated after the specified time-out period. The allowable range is 1-99 minutes. If not checked, the Internet connection will never be terminated.
Account User Name	Enter the account name provided by your ISP. This name will be used to log in to the ISP's server.
Password	Enter the current password for the above account. Re-enter the password in the *Verify* field to ensure it is correct.

IP Address from ISP	Select the appropriate option: • **Dynamic** This is the default, and the most common. Leave this selected if your ISP allocates an IP Address to the Wireless Router upon connection. • **Fixed IP Address** Select this if your ISP has allocated you a fixed IP Address, then enter the IP Address in the fields provided.
DNS IP Address	The DNS (Domain Name Server) translates names (e.g. microsoft.com) to IP Addresses. Enter the DNS IP address supplied or recommended by your ISP. If desired, additional DNS entries can be made on the *Options* screen.
Telephone	If using a Leased Line (permanent connection), ignore these fields. Otherwise, enter the telephone numbers to dial to connect to your ISP (Internet Service Provider). The first number is required; the others are optional. Enter the telephone numbers using the format described in your modem's user manual.
Dial-In	
Enable Dial-in	If checked, this port is available for dial-in access. Otherwise, any attempt to dial-in will be blocked. If Internet Access is also enabled, Dial-in users may find it difficult to connect because the telephone line is in use. Reducing the *Disconnect after Idle Time* setting for Internet Access to 1 minute may help. • See Dial -in Users later in this Chapter for details of creating and managing dial-in users. • See the *Dial-in* section in *Chapter 4 - PC Configuration* for details on setting up the remote PC to use the Wireless Router's Dial-in facility.
Disconnect after Idle Time	If checked, a Dial-in connection will be terminated after the specified time-out period. The allowable range is 1-99 minutes. If preferred, the connection time limit may be set individually for each user.
Dial-in PPP Link	Select the desired security option for log-in: • **PAP** has widespread support; almost all communications systems support it. • **CHAP** is more secure than PAP; the password is encrypted before transmission. If it is selected, the dial-in clients must also support CHAP in order to connect. • **MS CHAP** is the Microsoft version of CHAP, used on Windows platforms. If all dial-in clients are using Windows 95 or later, you can choose this option. • **None** means no login authentication is performed. **Warning!** If you choose "**None**", anyone can connect; this is a major security risk.
Links	
Dial-in Users	Use this link to create and manage users for the RAS Dial-in function. See the following section for details.

Status	Use this link to view the *Serial Port* status screen, described later in this chapter.

Modem Properties Screen

This screen will be displayed when the "Modem Properties" button on the ***Serial Port*** screen is clicked. Normally, it is not necessary to access this screen.

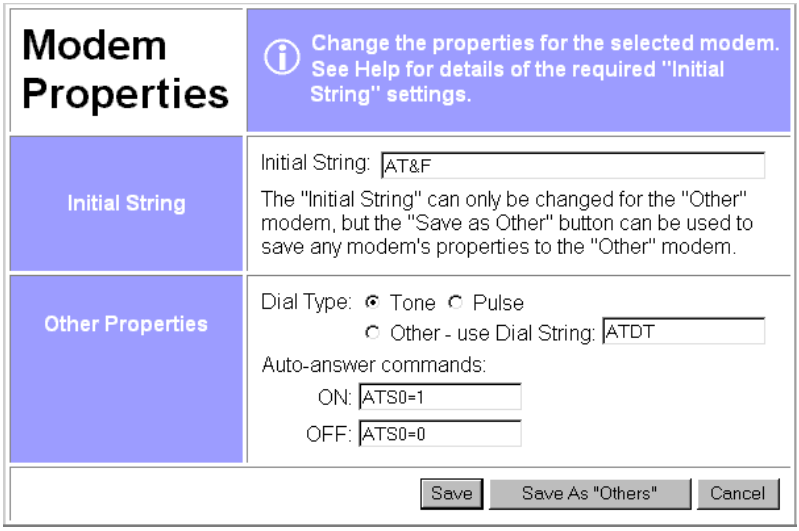

Modem Properties
Change the properties for the selected modem. See Help for details of the required "Initial String" settings.
Initial String
Initial String: AT&F
The "Initial String" can only be changed for the "Other" modem, but the "Save as Other" button can be used to save any modem's properties to the "Other" modem.
Other Properties
Dial Type: Tone Pulse
Other - use Dial String: ATDT
Auto-answer commands:
ON: ATS0=1
OFF: ATS0=0
Save
Save As "Others"
Cancel

Figure 20: Modem Properties Screen

Data – Modem Properties Screen

Initial String	
Initial String	This is a series of AT commands used to correctly configure your modem or ISDN. • The *Initial String* can only be changed for the "Other" modem type. • See **Appendix C - AT Commands** for further details about the required *Initial String* settings and standard AT commands.
Other Properties	
Dial Type	Select *Tone*, *Pulse* or *Other* to match your system. For *Other*, you must provide the ***Dial String***.
Dial String	The AT command sent to your modem before dialing. For example, "ATDT" tells your modem to use Tone Dialing. Check your modem's documentation to find the correct AT commands.
Auto Answer Commands	Enter the command strings which turn the "auto-answer" function in your modem or ISDN TA ON and OFF.
Buttons	
Save	Save the data on this screen. Note that if the current modem was not "Other" type, and you changed the *Initial String*, you can NOT use "Save". You must use "Save as Other" instead.

Save as "Other"	Assign the data shown on screen to the "Other" modem type, regardless of the modem selected on the ***Serial Port*** screen. You should then select "Other" as the Modem to use.
Cancel	Reverse any changes since the last "Save" operation.

Dial -in Users

This section describes how to create and manage remote users who wish to use the Wireless Router's RAS Dial-in facility.

For details of configuring the remote PC to use Dial-in access, refer to *Dial-in* in *Chapter 4 - Client PC Configuration*.

Overview

Once connected, the Dial-in user can access any LAN resources as if they were connected locally. This includes Internet access via the Wireless Router's WAN port.

The Wireless Router provides the following options to control Dial-in access:

1. Allow access by anyone and everyone.
   - If Dial-in PPP link security on the Serial Port screen is set to "None", then the user name and password is not checked, so anyone who dials in can gain access.
   - This creates a major security weakness. It is strongly recommended that this option is NOT used.
2. All users use the same log-in.
   - All Dial-in users can use the existing "guest" user, once Dial-in access is Enabled for both the Serial port and the *guest* user.
   - A password should be assigned to the "guest" user. By default, there is no password.
3. Each Dial-in user has a separate log-in and password
   - This is the recommended approach.
   - Each person requiring dial-in access is entered in the Wireless Router's user database, using the ***Dial-in Users*** and ***User Details*** screens.

Dial-in Users Screen

This screen is reached via the *Dial-in Users* link on the ***Serial Port*** screen.

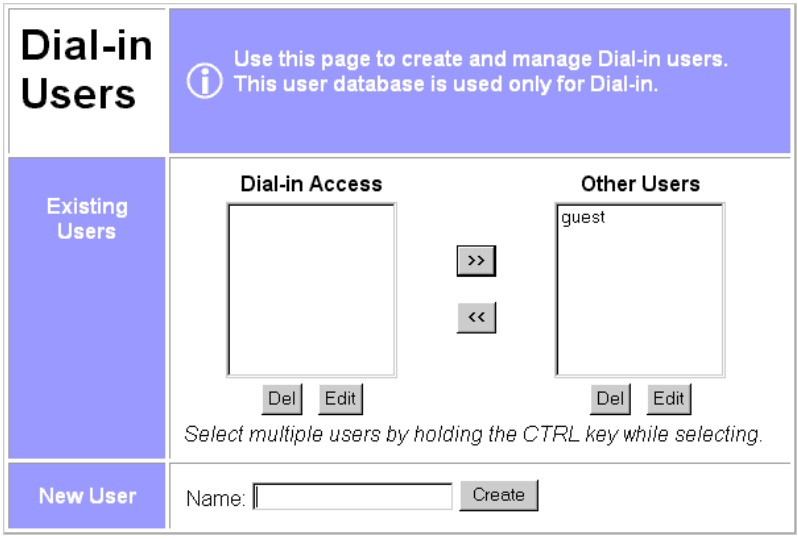


Figure 21: Dial-in Users Screen

Data – Dial-in Users Screen

Existing Users	
Dial-in Access	• This lists all users who have Dial-in permission. • If no users have dial-in permission, this list will be empty. • Select the user or users you wish to change. Multiple users can be selected by holding down the CTRL key while selecting. (For the Macintosh, use the SHIFT key instead of CTRL).
Other Users	• This lists all users who do not have Dial-in access. • If you have not created any users, this list will contain the pre-defined "guest" user. • Use the "Create" button on this screen to create new users as required. • Select the user or users you wish to change. Multiple users can be selected by holding down the CTRL key while selecting. (For the Macintosh, use the SHIFT key instead of CTRL).
New User	
Name	Use this to create new users as required: • Enter the name for the new user here. • Spaces, punctuation, and special characters must NOT be used in the name. • User names are case insensitive (case is ignored), so you can not have 2 names which differ only by case. • The name can not be changed once the user is created.

Buttons	
>>	Use the " >> " button to remove Dial-in access for any users selected in the "Dial-in Users" list.
<<	Use the " << " button to allow Dial-in access for any users selected in the "Other Users" list.
Del	Delete the selected user or users in the list above the button.
Edit	Modify the selected user in the list above the button. Only 1 user should be selected.
Create	This will add a new user to the database. • Enter the required user name in the "Name" field, then click the *Create* button. • You will then see the "User Details" screen, where you can enter the other details for this user.

User Details Screen

This screen is displayed in the following situations:

- Either of the *Edit* buttons on the ***Dial-in Users*** screen is used to modify the selected user.
- The *Create* button on the ***Dial-in Users*** screen is used to create a new user.

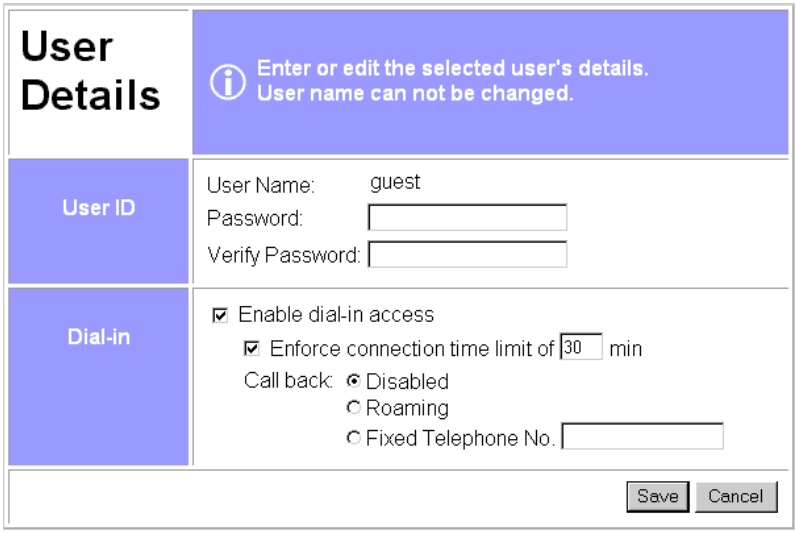


Figure 22: User Details Screen

Data – User Details Screen

User ID	
User Name	The user name can not be changed.
Password **Verify Password**	The password for the current user. Passwords are case sensitive. When creating or changing a password, enter it in the *Verify Password* field also.

Dial-in	
Enable dial-in access	Use this to suspend or enable dial-in access. This setting can also be changed on the ***Dial-in Users*** screen.
Enforce connection time limit	If checked, the Wireless Router will terminate the Dial-in connection after the specified period. The time period can be set from 1 to 999 minutes. If unchecked, the connection time-out set on the *Serial Port* screen will be used. If neither time-out is enabled, the connection must be terminated by the remote user.
Call back	Select the desired option: • **Disabled**:- The user can simply dial-in; the Wireless Router will not hang-up and call back. • **Roaming**:- After providing their name and password, the user is prompted for the call-back number. The Wireless Router will then hang up and dial the number provided by the remote user. • **Fixed**:- The number entered in the **Telephone No.** field is always used as the call-back number. The Wireless Router will accept the incoming call, authenticate the user, then hang up and dial this number. • **Telephone No**:- If *Fixed* is chosen, a telephone number must be entered in this field. For the other options, this field is ignored.

Serial Port Status

This screen is reached by either of the following:

- **Status Screen** - *Serial Port Status* link
- **Serial Port Screen** - *Status* link.

An example screen is shown below.

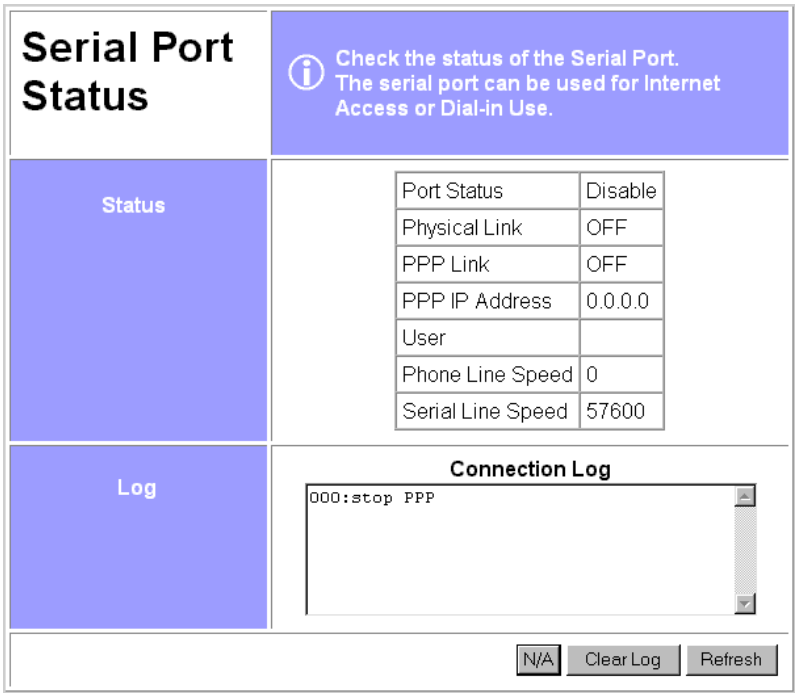


Figure 23: Serial Port Status Screen

Overview

- **Status** - This section displays the current connection status for the serial port connection.
- **Dial/HangUp Button** - This button will display *Dial* if there is no connection and *Hang-up* if a connection exists. Use this to dial the ISP, or terminate an existing connection. If the Serial Port is Disabled, this button will display "N/A".
- **Clear Log Button** - Clicking this button clears all messages in the log, making new messages easier to read.
- **Refresh Button** - Use this to update the data on screen.

Data - Serial Port Status Screen

Status	
Port Status	This shows the current port operation. Possible values are: • Internet Access • Dial-in • Idle • Disabled "Disabled" indicates neither Internet Access nor Dial-in is Enabled.

Physical Link	If operating, the link will show ON. This means the modem was able to connect to the number dialed.
PPP Link	If ON, a PPP connection was successfully negotiated.
PPP IP Address	This has 2 possible meanings, depending of the type of connection: • **Internet Access** - This is the IP Address used by this device, as seen by Internet users. This address is provided by your ISP. • **Dial-in** - This is the IP Address used by the remote user. This IP Address is allocated by the DHCP Server function in the Wireless Router.
User	There are 2 possibilities: • For Internet Access, this shows the Internet Account name. • For Dial-in operations, this shows the current user.
Phone Line Speed	The connection speed over the phone line, between your modem and the number dialed, as reported by your modem.
Serial Line Speed	The connection speed between this device and the modem. This setting can be changed on the *Serial Port* screen.
Log	
Connection Log	This displays connection details. See below for a description of the most common items in this log.

Connection Log

This shows the commands sent to the modem, and any status messages returned by the modem. Note that you must click *Refresh* to update the information.

The following table lists the common messages, and their meaning.

Message	Description
Dialing	Dialing the ISP
Try to establish physical connection.	The device is trying to connect with the ISP, using the modem.
Busy	The number dialed was busy.
Physical line is connected	Physical connection to ISP has been established.
CONNECT *nnnnnn*	Physical connection was successful; *nnnnnn* indicates the speed of the serial link as currently configured.
Max phone line speed *nnnnnn* bps	*nnnnnn* is the maximum speed of the modem, according to the current configuration.
DCD low, DSR low	Physical line break, connection lost.
send "-----" wait "-----"	"AT" commands sent to the modem are displayed as they are sent. Commands in the Script file are also displayed as they are executed.

Start PPP	Having established a physical connection, a PPP connection is now being established.
PPP up fail	The PPP connection could not be established.
PPP up successfully	The PPP connection was established successfully.
Stop PPP	The PPP connection was terminated. This will occur at the end of a session, or an error condition.
Try to hang up	Attempting to get the modem to hang up.
Time out	There was no response from the modem
No carrier No answer	The number dialed did not answer.
Idle timer expires	"Disconnect after Idle Time" is Enabled, and the Time-out period has been reached. The connection will now be terminated..
No dial tone	The modem could not obtain a dial tone.
Set baudrate nnnn	The serial line speed is being set to the speed set in the configuration.

Chapter 7
Options

This Chapter details the options available on the Wireless Router's "Options" screen.

Overview

An example Options screen is shown below.

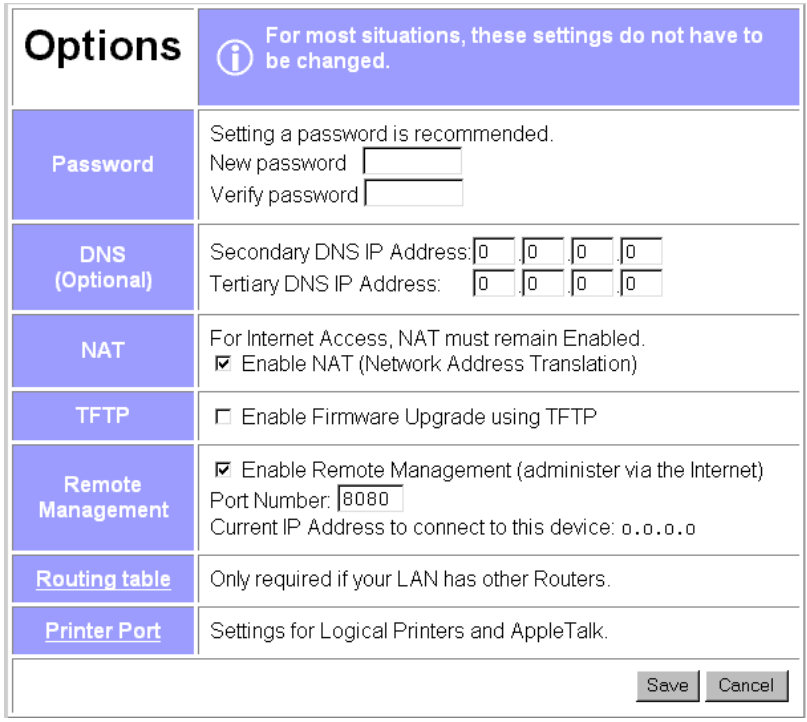

Options
For most situations, these settings do not have to be changed.
Password
Setting a password is recommended.
New password
Verify password
DNS (Optional)
Secondary DNS IP Address: 0 .0 .0 .0
Tertiary DNS IP Address: 0 .0 .0 .0
NAT
For Internet Access, NAT must remain Enabled.
Enable NAT (Network Address Translation)
TFTP
Enable Firmware Upgrade using TFTP
Remote Management
Enable Remote Management (administer via the Internet)
Port Number: 8080
Current IP Address to connect to this device: 0.0.0.0
Routing table
Only required if your LAN has other Routers.
Printer Port
Settings for Logical Printers and AppleTalk.
Save
Cancel

Figure 24: Options Screen

Password

Once a password is entered, it is required in order to change the device configuration. Passwords are case sensitive and can be up to 8 alphanumeric characters (no spaces or punctuation).

To create or change the password, enter the required password in both the *New Password* and *Verify Password* input fields.

When prompted for the password, leave the "User Name" blank.

DNS (Domain Name Server

- These entries are optional. The main DNS (Domain Name Server) is either provided by your ISP, or entered on the *Quick Setup* screen.
- If desired, enter any other DNS IP Addresses here. The first available DNS will be used.

NAT (Network Address Translation)

NAT allows PCs on your LAN to share a single external (Internet) IP Address. This IP Address is supplied by your ISP. Use the following to determine whether or nor you need NAT.

- For Internet access, NAT **must be left On** unless all PCs on your LAN have valid external IP Addresses.
- If this device is not being used to provide shared Internet access, NAT is not normally required. With NAT disabled, the Wireless Router will act as a static router.
- If NAT is disabled, the Firewall protection provided by the Wireless Router is lost, and the *Advanced Internet* features (Virtual Servers, Special Applications, and DMZ) are no longer available.

TFTP

TFTP (Trivial FTP) can be used to upgrade the firmware in the Wireless Router. However, this is not normally required; there is a Windows utility available for this purpose.

Remote Management

This feature allows you to manage the Wireless Router via the Internet.

Enable Remote Management	Enable to allow management via the Internet. If Disabled, this device will ignore management connection attempts from the WAN port.
Port Number	Enter a port number between 1024 and 65535 (8080 is recommended). This port number must be specified when you connect (see below). **Note:** The default port number for HTTP (Web) connections is port 80, but using port 80 here will prevent the use of a Web "Virtual Server" on your LAN. (See *Advanced Internet - Virtual Servers*)
Current IP Address	You must use this IP Address to connect (see below). This IP Address is allocated by your ISP. But if using a Dynamic IP Address, this value can change each time you connect to your ISP. So it is better if your ISP allocates you a Fixed IP Address.

To connect from a remote PC via the Internet

1. Ensure your Internet connection is established, and start your Web Browser.

2. In the "Address" bar, enter "HTTP://" followed by the WAN IP Address of the Wireless Router. If the port number is not 80, the port number is also required. (After the IP Address, enter ":" followed by the port number.)
   e.g.
   `HTTP://123.123.123.123:8080`

   This example assumes the WAN IP Address is 123.123.123.123, and the port number is 8080.

Routing Table

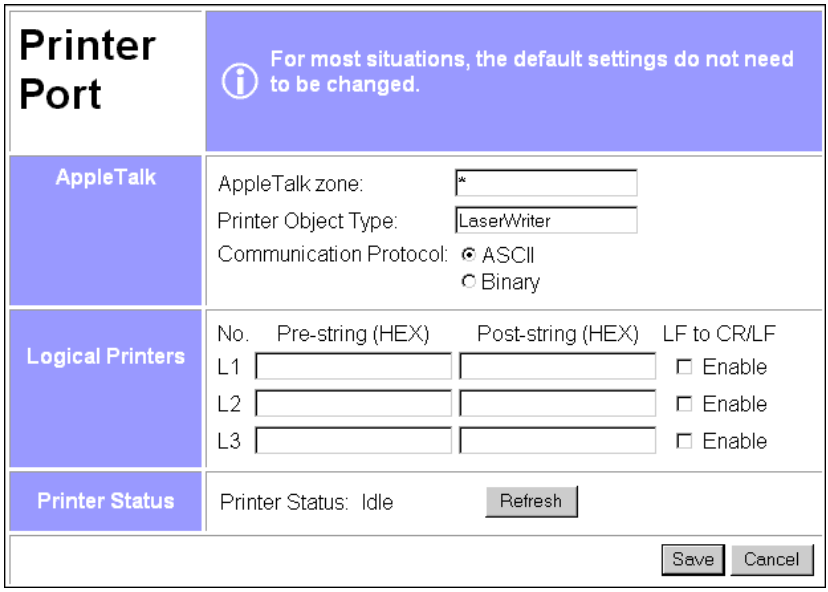
This link provides access to a standard static routing table.

Configuration is only required if your LAN contains other routers.

Refer to *Chapter 8 - Routing* for further details about Router configuration and using the *Router* screen.

Printer Port

This link will reveal the ***Printer Port*** screen, as shown below. Most users do not need to change these settings.



Printer Port Screen

Data - Printer Port Screen

AppleTalk	
AppleTalk Zone	This determines which Apple systems can gain access to this printer. The default value is *, which allows access by all systems. If you enter another zone name, only Apple systems in that zone will be able to access the printer.

Printer Object Type	Sets the type of printer attached. The default setting is "Laser-Writer". If the attached printer is not a LaserWriter (or compatible), then you must: • Install the correct printer driver for the printer on each Apple system requiring printer access • Check your Printer's user manual or manufacturer's Web site and find the correct "Printer Object Type" • Enter the correct "Printer Object Type" on this screen. If the "Printer Object Type" is incorrect, the printer will not be visible from your Apple system.
Communication Protocol	You must use the same setting as your Macintosh.
Logical Printers	
No (L1, L2, L3)	There are 3 Logical Printers (Ports), named L1, L2, and L3. These names can not be changed, and must be used when selecting the logical printer from your Unix system.
Pre-string (HEX)	Enter (in HEX) the series of printer commands to be sent to the attached printer BEFORE each print job.
Post-string (HEX)	Enter (in HEX) the series of printer commands to be sent to the attached printer AFTER each print job.
LF to CR/LF	If checked, Unix-style LF (line feed) characters at the end of each line will be converted to CR/LF (carriage return/line feed) pairs, as used in MSDOS and Windows.
Printer Status	
Printer Status	This indicates the current status of the printer. Possible values are: • Idle • Printing • Off-line • Out of paper
"Refresh" Button	Click this to update the printer status information

Chapter 8
Routing

This Chapter explains the Routing features of the Wireless Router.

Overview

- If you don't have other Routers or Gateways on your LAN, ignore the "Routing" page completely.
- If the Wireless Router is only acting as a Gateway for the local LAN segment, ignore the "Routing" page even if your LAN has other Routers.
- If your LAN has a standard Router (e.g. Cisco) on your LAN, and the Wireless Router is to act as a Gateway for all LAN segments, enable RIP (Routing Information Protocol) and ignore the Static Routing table.
- If your LAN has other Gateways and Routers, and you wish to control which LAN segments use each Gateway, do NOT enable RIP (Routing Information Protocol). Configure the Static Routing table instead. (You also need to configure the other Routers.)
- If using Windows 2000 Datacenter Server as a software Router, enable RIP on the Wireless Router, and ensure the following Windows 2000 settings are correct:
  - Open *Routing and Remote Access*
  - In the console tree, select *Routing and Remote Access , [server name], IP Routing, RIP*
  - In the "Details" pane, right-click the interface you want to configure for RIP version 2, and then click "Properties".
  - On the "General" tab, set *Outgoing packet protocol* to "RIP version 2 broadcast", and *Incoming packet protocol* to "RIP version 1 and 2".

Routing Screen

The routing table is accessed by the *Routing* link on the ***Options*** screen.

Using this Screen

Generally, you will use either RIP (Routing Information Protocol) OR the Static Routing Table, although is it possible to use both methods simultaneously.

Static Routing Table

If RIP is not used, an entry in the routing table is required for each LAN segment on your Network, other than the segment to which this device is attached.

The other Routers must also be configured. See Router Configuration later in this chapter for further details and an example.

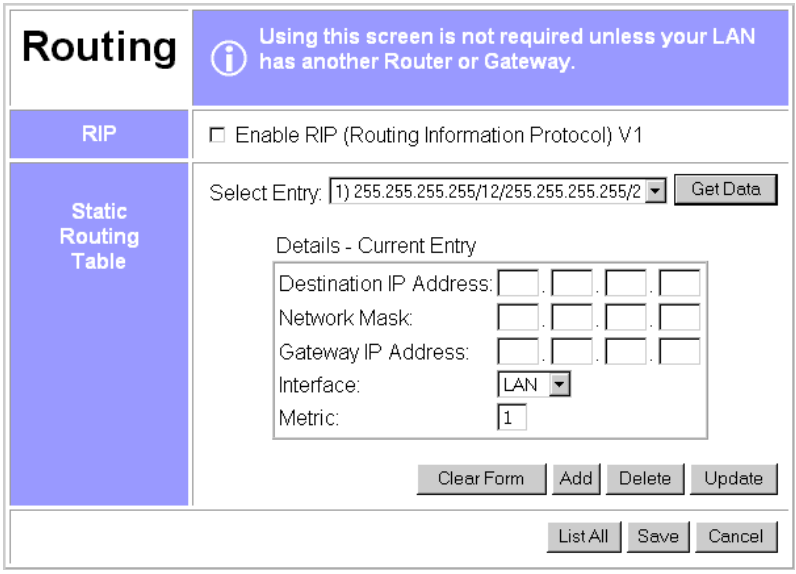


Figure 25: Routing Screen

Data - Routing Screen

RIP	
Enable RIP	Check this to enable the RIP (Routing Information Protocol) feature of the Wireless Router. The Wireless Router supports RIP 1 only.
Static Routing Table	
Select Entry	This drop-down list shows all entries in the Routing Table. • To view or change an entry, select it, then click the *Get Data* button. • After making any required changes, click the *Update* button to save your changes.
Destination IP Address	The network address of the remote LAN segment. For standard class "C" LANs, the network address is the first 3 fields of this *Destination IP Address*. The 4th (last) field can be left at 0.
Network Mask	The Network Mask used on the remote LAN segment. For class "C" networks, the standard Network Mask is 255.255.255.0
Gateway IP Address	The IP Address of the Router on the LAN segment to which this device is attached. (NOT the router on the remote LAN segment.)
Interface	Select the appropriate interface - LAN (Internal LAN) or WAN (External LAN or WAN) from the drop-down list.
Metric	The number of routers which must be traversed to reach the remote LAN segment. The default value is 1.
Buttons	
Clear Form	Clears all data, ready for input of a new entry.
Add	Add a new entry to the Routing table, using the data shown on screen. The name shown in the drop-down list is ignored.

Delete	Delete the entry selected in the drop-down list, regardless of whether its details are shown on screen.
Update	Update the entry selected in the drop-down list, using the data shown on screen.
List All	List all entries in the Routing table.
Save	Save the RIP setting. This has no effect on the Static Routing Table.
Cancel	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

Router Configuration

It is essential that all IP packets for devices not on the local LAN be passed to the Wireless Router, so that they can be forwarded to the external LAN, WAN, or Internet. To achieve this, the local LAN must be configured to use the Wireless Router as the *Default Route* or *Default Gateway*.

Local Router

The local router is the Router installed on the same LAN segment as the Wireless Router. This router requires that the *Default Route* is the Wireless Router itself. Typically, routers have a special entry for the *Default Route*. It should be configured as follows.

Destination IP Address	Normally 0.0.0.0, but check your router documentation.
Network Mask	Normally 0.0.0.0, but check your router documentation.
Gateway IP Address	The IP Address of the Wireless Router.
Metric	1

Other Routers on the Local LAN

Other routers on the local LAN must use the Wireless Router's *Local Router* as the *Default Route*. The entries will be the same as the Wireless Router's local router, with the exception of the *Gateway IP Address*.

- For a router with a direct connection to the Wireless Router's local Router, the *Gateway IP Address* is the address of the Wireless Router's local router.
- For routers which must forward packets to another router before reaching the Wireless Router's local router, the *Gateway IP Address* is the address of the intermediate router.

Static Routing - Example

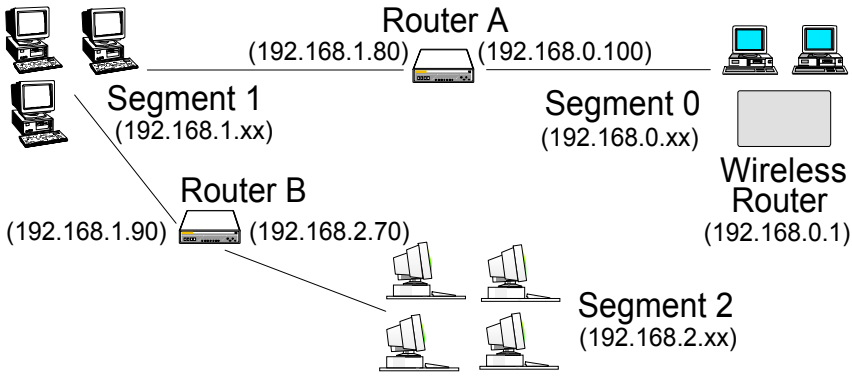


Figure 26: Routing Example

For the Wireless Router's Routing Table

For the LAN shown above, with 2 routers and 3 LAN segments, the Wireless Router requires 2 entries as follows.

Entry 1 (Segment 1)	
Destination IP Address	192.168.1.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100 (Wireless Router's local Router)
Interface	LAN
Metric	1
Entry 2 (Segment 2)	
Destination IP Address	192.168.2.0
Network Mask	255.255.255.0 (Standard Class C)
Gateway IP Address	192.168.0.100
Interface	LAN
Metric	2

For Router A's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.0.1 (Wireless Router's IP Address)

For Router B's Default Route

Destination IP Address	0.0.0.0
Network Mask	0.0.0.0
Gateway IP Address	192.168.1.80 (Wireless Router's local router)

Chapter 9
Advanced Internet

9

This Chapter explains how to use the Wireless Router's "Advanced Internet" features.

Overview

For situations where the Wireless Router is being used to provide shared Internet access, the following advanced features are provided.

- Special Internet Applications
- URL Filter
- Virtual Servers
- DMZ

This chapter contains details of the configuration and use of each of these features.

Advanced Internet Screen

This screen provides access to the advanced Internet features, and provides a convenient overview and control center. An example screen is shown below.

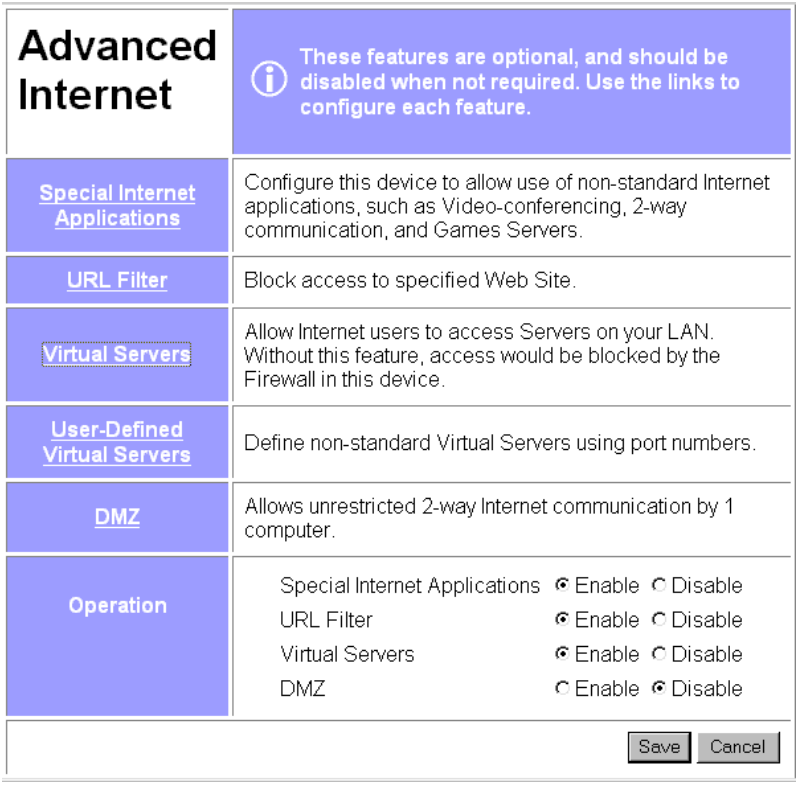

Advanced Internet
These features are optional, and should be disabled when not required. Use the links to configure each feature.
Special Internet Applications
Configure this device to allow use of non-standard Internet applications, such as Video-conferencing, 2-way communication, and Games Servers.
URL Filter
Block access to specified Web Site.
Virtual Servers
Allow Internet users to access Servers on your LAN. Without this feature, access would be blocked by the Firewall in this device.
User-Defined Virtual Servers
Define non-standard Virtual Servers using port numbers.
DMZ
Allows unrestricted 2-way Internet communication by 1 computer.
Operation
Special Internet Applications Enable Disable
URL Filter Enable Disable
Virtual Servers Enable Disable
DMZ Enable Disable
Save
Cancel

Figure 27: Advanced Internet Screen

On this screen, you can enable or disable any required feature.

Special Internet Applications

This feature is only required if you wish to use Internet applications which require 2-way communication, multiple connections, or combined TCP/UDP connections.

Examples of such applications are Internet Videoconferencing, Telephony, Games Servers, and other special-purpose Servers.

Generally, you will become aware of the need for this feature when an Internet application is unable to function correctly.

At any time, only one (1) PC can use each Special Application.

Special Applications Screen

This screen can be reached by selecting *Special Internet Applications*. An example screen is shown below.

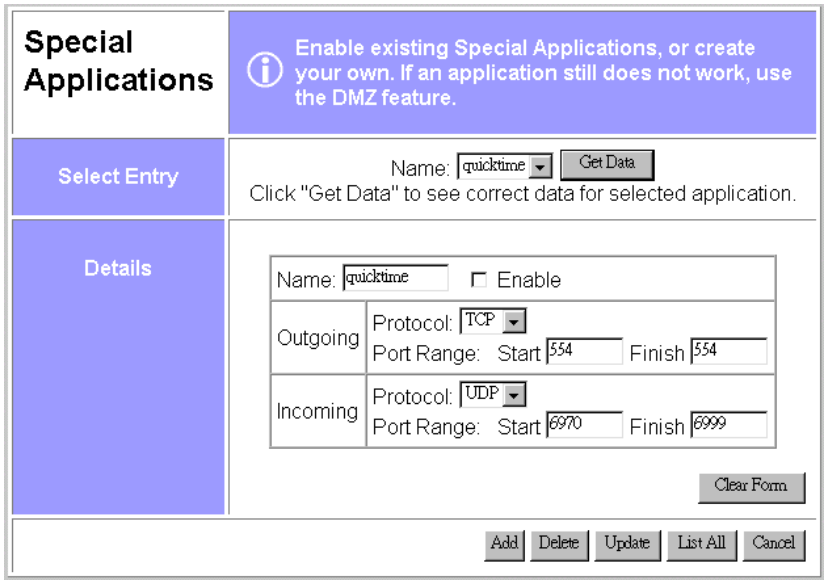


Figure 28: Special Applications Screen

Using a Special Application

- Ensure that *Special Applications* has been enabled on the *Advanced Internet* screen.
- Configure the *Special Applications* screen as required.

Configuration data must be obtained from the Service/Application provider.

If an application still cannot function correctly, try using the "DMZ" feature.

Some Special Applications have been defined but not enabled.

Managing Special Application Entries

Enable	1. Select the entry from the drop-down list 2. Click "Get Data" 3. Check the *Enable* checkbox 4. Click "Update"
Disable	As above, but uncheck the *Enable* checkbox.
Disable all	On the *Advanced Internet* screen, you can Enable or Disable the *Special Applications* feature.
Delete	1. Select the entry from the drop-down list 2. Click "Delete"
Modify (Edit)	1. Select the entry from the drop-down list 2. Click "Get Data" 3. Make any desired changes 4. Click "Update"
Create a new entry	1. Click "Clear Form" 2. Enter the required data, as described below. 3. Click "Add".

Data - Special Applications Screen

This data must be obtained from the service provider.

Select Entry	
Name	This drop-down list shows all *Special Applications* which have been defined.
Get Data Button	After selecting the desired entry, click this button to view its current settings in the *Details* section of the screen. You can then make any changes required. Click the "Update" button to save your changes.
Details	
Name	Enter a descriptive name to identify this application entry.
Enable	Use this to Enable or Disable support for this application, as required.
Outgoing	
Protocol	The protocol (TCP or UDP) used when you connect to the special application service.
Port Range: Start	The beginning of the range of port numbers used by the application server, for data you send to it. If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, for data you send.

Incoming	
Protocol	The protocol (TCP or UDP) used when the application or service sends data to you.
Port Range: Start	The start of the range of port numbers used by the application server when data is sent to you. If using only one port number, enter it in both the "Start" and "Finish" fields.
Port Range: Finish	The end of the range of port numbers used by the application server, when data is sent to you.
Buttons	
Clear Form	Clears all data, ready for input of a new entry.
Add	Add a new entry to the Special Applications database, using the data shown on screen. The name shown in the drop-down list is ignored.
Delete	Delete the Special Application entry selected in the drop-down list, regardless of whether its details are shown on screen.
Update	Update the Special Application entry selected in the drop-down list, using the data shown on screen.
List All	List all Special Application entries.
Cancel	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

URL Filter

The *URL Filter* provides a means to block access to undesirable Web sites. The blocking action applies to all PCs accessing the Internet via the Wireless Router.

Operation

The *URL Filter* feature works by matching the "Filter Strings" (text strings) against the requested URL. For example, by inputting the word “bad” in the *URL Filter*, any URL containing the letters “bad” in it will be blocked.

Note that if **any component** of the URL request contains one of the "Filter Strings", that request will be blocked while the *URL Filter* is enabled.

URL requests to Web (Internet) Servers include the following components:

- **Protocol.** For Internet access, the usual protocol is HTTP (shown in your browser as "HTTP://"). The URL Filter works ONLY with the HTTP protocol. Other protocols, such as FTP and E-Mail, are not affected by the URL Filter.
- **Domain.** This is the address of the site (e.g. www.microsoft.com)
- **Path.** This specifies a certain file on the Server (e.g. /public/docs/index.html)
- **Parameters.** This is the data which is sent (submitted) to the Server when you submit a form, such as when you use a search engine to search the Internet.
  On a Web page, clicking a link may also submit data to a Server, rather than just request a file.

All of these components are searched to see if they contain any of the "Filter Strings".

Tips

- To use the *URL Filter* feature properly, you should try inputting as much of the text for the given URL as possible. For example, instead of simply using the word “bad,” you could use the full web site name.
- If you do not want to block an entire web site, you can include the path rather than just the domain. For example, “www.badsite.com/badsection/”
- Be careful when using the *URL Filter*, as a general word might block access to many other sites as well as the one that you intend to block.
- You can use the *Internet Access Log*, accessed from the ***Status*** screen, to see which sites have been blocked by the *URL Filter*.

URL Filter Screen

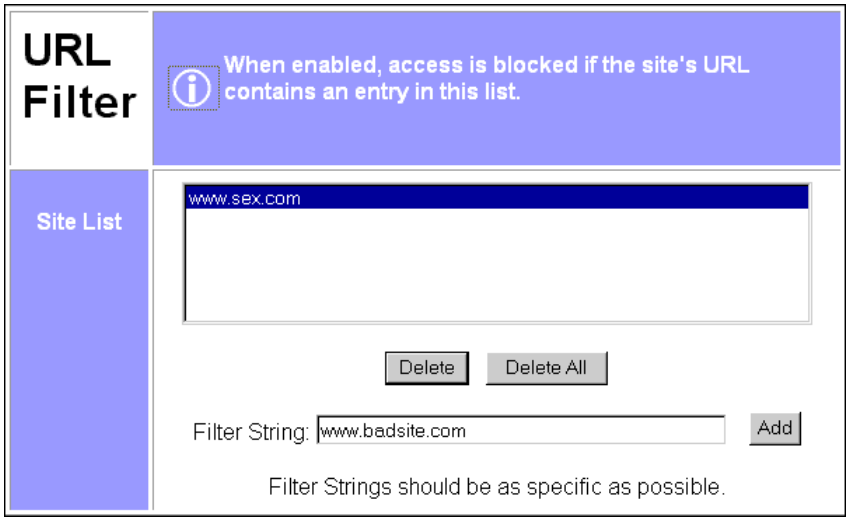


Figure 29: URL Filter Screen

Data - URL Filter Screen

Site List	
Site List	This lists any existing entries. If you have not entered any values, this list will be empty.
Filter String	To add an entry to the list, enter it here, and click the "Add" button. An entry may be a Domain name (e.g. www.trash.com) or simply a string (e.g. ads/) Any URL which contains ANY entry ANYWHERE in the URL will be blocked.
Buttons	**Delete/Delete All** - Use this buttons to delete the selected entry or all entries, as required. Multiple entries can be selected by holding down the CTRL key while selecting. (On the Macintosh, hold the SHIFT key while selecting.) **Add** - Use this to add the current *Filter String* to the site list.

You can use the *Internet Access Log*, accessed from the *Status* screen, to see which sites have been blocked by the URL Filter.

Virtual Servers

This feature allows you to make Servers on your LAN accessible to Internet users. Normally, Internet users would not be able to access a server on your LAN because:

- Your Server does not have a valid external IP Address.
- Attempts to connect to devices on your LAN are blocked by the firewall in this device.

The "Virtual Server" feature solves these problems and allows Internet users to connect to your servers, as illustrated below.

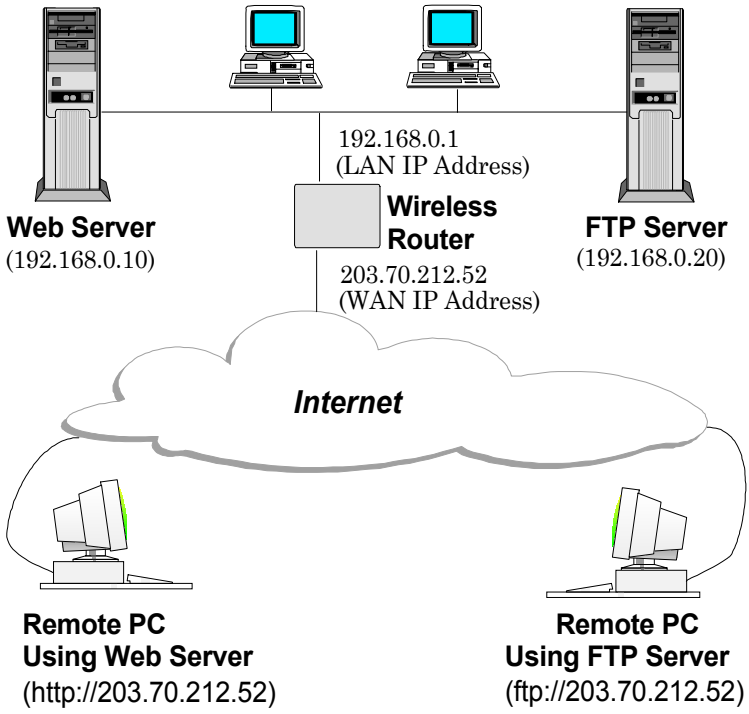


Figure 30: Virtual Servers

IP Address seen by Internet Users

Note that, in this illustration, both Internet users are connecting to the same IP Address, but using different protocols.

To Internet users, all virtual Servers on your LAN have the same IP Address. This IP Address is allocated by your ISP.

This address should be static, rather than dynamic, to make it easier for Internet users to connect to your Servers. If using a Static IP Address, it is entered on the "WAN" screen.

Types of Virtual Servers

The Wireless Router supports two (2) types of Virtual Servers:

- **Pre-defined** - Standard server types. The only data required is the IP Address of the server on your LAN.
- **User-defined** - Non-standard servers. You must provide additional information about the server.

Note: The TOTAL number of Virtual Servers which can be used at any time is 10.

Virtual Server Screen

The *Virtual Servers* screen is reached by the *Advanced Internet - Virtual Servers* link.

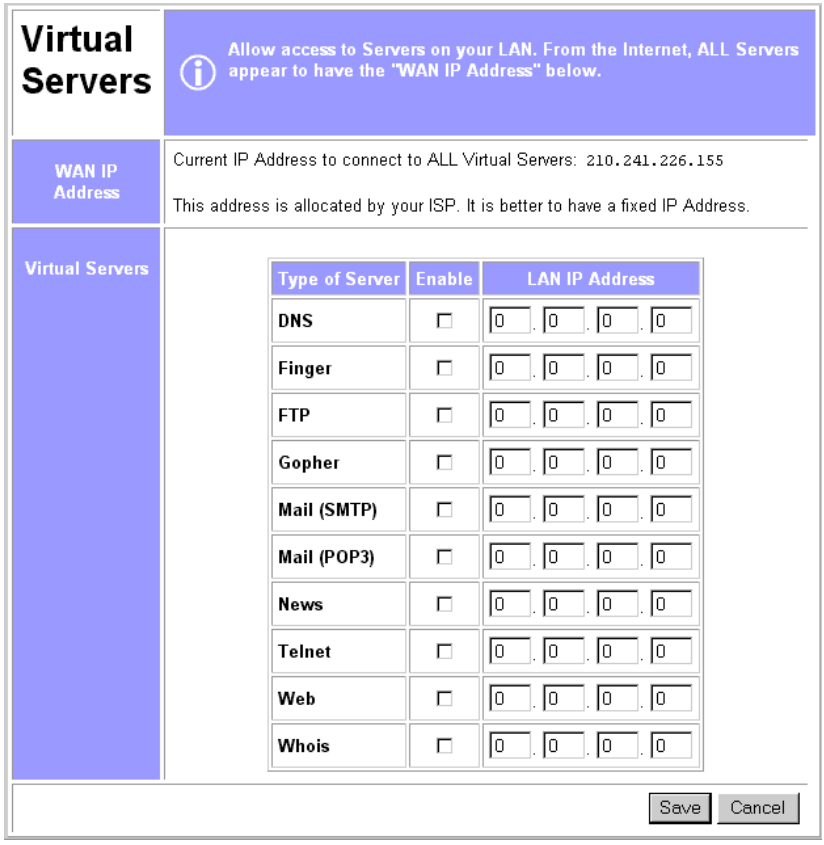


Figure 31: Virtual Server Screen.

Data – Virtual Server Screen

WAN IP Address	
Current IP Address	This shows the IP Address which Internet users must use to connect to any of your Virtual Servers. • To Internet Users, ALL of your Virtual Servers have the same IP Address. • This IP Address is allocated by your ISP. It is better to have a fixed IP Address.
Virtual Servers	
Type	Select the type of Server you wish to use.
Enable	Check to enable this Server.

LAN IP Address	• Enter the IP Address of a PC on your LAN.
	• You must install and configure the appropriate Server software on the PC entered here.
	• If using DHCP, the LAN IP Address of a PC may change. To solve this problem, use either of these methods:
	  • Assign a fixed IP Address to the Server PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server.
	  • Reserve an IP Address for the Server PC in the DHCP Server, using the *Access Control - PC* screen.

For each entry, the PC must be running the appropriate Server software.

User Defined Virtual Servers

If the type of Server you wish to use is not listed on the *Virtual Servers* screen, you can define it using this feature.

Select *Advanced Internet - User Defined Virtual Servers* to see a screen like the example below.

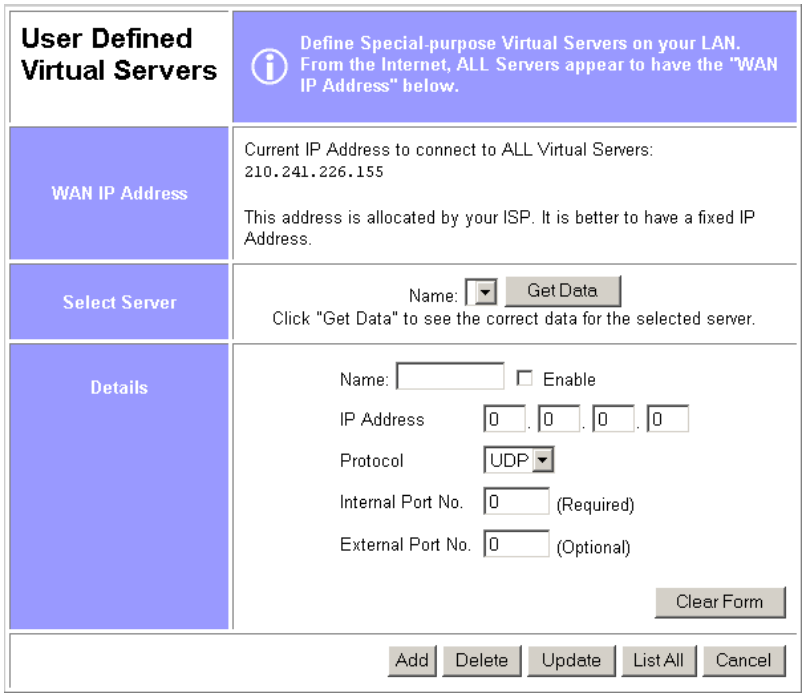


Figure 32: User Defined Virtual Servers

Managing User Defined Virtual Servers

Enable a Server	1. Select the required entry from the drop-down list 2. Click "Get Data" 3. Check the *Enable* checkbox 4. Click "Update"
Disable a Server	As above, but uncheck the *Enable* checkbox.
Disable all Servers	On the *Advanced Internet* screen, you can Enable or Disable the *Virtual Servers* feature.
Delete	1. Select the entry from the drop-down list 2. Click "Delete"
Modify (Edit)	1. Select the entry from the drop-down list 2. Click "Get Data" 3. Make any desired changes 4. Click "Update"
Create a new entry	1. Click "Clear Form" 2. Enter the required data, as described below. 3. Click "Add".

Data- User Defined Virtual Servers Screen

WAN IP Address	
Current IP Address	This shows the IP Address which Internet users must use to connect to any of your Virtual Servers. • To Internet Users, ALL your Virtual Servers have the same IP Address. • This IP Address is allocated by your ISP. It is better to have a fixed IP Address.
Select Server	
Name	This lists any Servers you have defined. Click the "Get Data" button to view the correct data for the selected Server.
Get Data Button	After selecting the desired entry, click this button to view its current settings in the *Details* section of the screen. You can then make any changes required. Click the "Update" button to save your changes.
Details	
Name	Enter a descriptive name to identify this Server entry.
Enable	Use this to Enable or Disable support for this Server, as required.
IP Address	The IP Address of the PC on your LAN which is running the Server software.
Protocol	Select the protocol (TCP or UDP) used by the Server.

Internal Port Number	Enter the port number used by the Server to connect to clients.
External Port Number	The port number used by clients when connecting to the Server. This is normally the same as the *Internal Port Number*. If it is different, this device will perform a "mapping" or "translation" function, allowing the server to use one port address, while clients use a different port address.
Buttons	
Clear Form	Clears all data, ready for input of a new entry.
Add	Add a new entry, using the data shown on screen. The name shown in the drop-down list is ignored.
Delete	Delete the Virtual Server entry selected in the drop-down list, regardless of whether its details are shown on screen.
Update	Update the Virtual Server entry selected in the drop-down list, using the data shown on screen.
List All	List all User-defined Virtual Servers.
Cancel	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

From the Internet, ALL Virtual Servers have the IP Address allocated by your ISP, as shown by the "WAN IP Address".

Connecting to the Virtual Servers

Once configured, anyone on the Internet can connect to your Virtual Servers. They must use the WAN Port IP Address (the IP Address allocated to this device by your ISP).
e.g.

```
http://203.70.212.52
ftp://203.70.212.52
```

It is more convenient if you are using a Fixed IP Address from your ISP, rather than Dynamic. If using a Fixed IP Address, it is entered on the *WAN* screen.

DMZ

This feature, if enabled, allows one (1) computer on your LAN to be exposed to all users on the Internet, allowing unrestricted 2-way communication between the "DMZ" PC and other Internet users or Servers.

This allows connection to special-purpose servers which require proprietary client software, or 2-way user connections such as Video-conferencing, which requires both users to run special software.

To allow unrestricted access, the Firewall in this device is disabled, creating a security risk.

You should use this feature only if the "Special Applications" feature is insufficient to allow an application to function correctly. This feature should be turned ON only when needed, and left OFF the rest of the time.

DMZ Screen

Select *Advanced Internet* from the navigation bar, then *DMZ*. You will see a screen like the following:

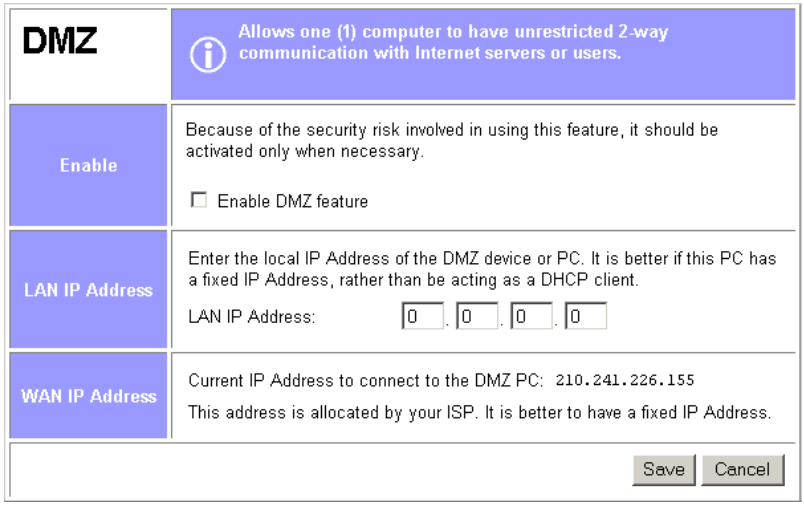

DMZ
Allows one (1) computer to have unrestricted 2-way communication with Internet servers or users.
Enable
Because of the security risk involved in using this feature, it should be activated only when necessary.
Enable DMZ feature
LAN IP Address
Enter the local IP Address of the DMZ device or PC. It is better if this PC has a fixed IP Address, rather than be acting as a DHCP client.
LAN IP Address: 0 . 0 . 0 . 0
WAN IP Address
Current IP Address to connect to the DMZ PC: 210.241.226.155
This address is allocated by your ISP. It is better to have a fixed IP Address.
Save
Cancel

Figure 33: DMZ Screen

Data – DMZ Screen

Enable	
Enable DMZ Feature	Use this to Enable or Disable the DMZ feature. The DMZ feature should be disabled when not required.
LAN IP Address	
LAN IP Address	Enter the IP Address of the PC on your LAN which will become the "DMZ" PC. If using DHCP, the LAN IP Address of a PC may change. To solve

	this problem, you can use either of these methods: • Assign a fixed IP Address to the DMZ PC, ensuring that its IP Address is NOT within the address range allocated by the DHCP Server. • Reserve an IP Address for the DMZ PC in the DHCP Server, using the *Access Control - PC* screen.
WAN IP Address	
WAN IP Address	This is the IP Address that Internet users must use to connect to the "DMZ" PC. This IP Address is allocated by your ISP. It is better if you are using a fixed IP Address, so that it never changes. This will make it easier for Internet users to connect to you. If using a Static IP Address, it is entered on the "WAN" screen.

To Internet users, the IP Address of the DMZ computer is the IP Address allocated by your ISP, as shown by the "WAN IP Address".

Chapter 10
Access Control

10

This Chapter explains how to configure and use the Wireless Router's "Access Control" feature.

Overview

The Access Control feature allows administrators to restrict Internet Access by individual PCs. The process uses "Packet Filtering" to block or discard data packets. By default, no packets are blocked or discarded.

To use this feature:

- Set the desired restrictions on the "Everyone" group. All PCs are in the "Everyone" group unless explicitly moved to another group, using the *PC* screen.
- Set the desired restrictions on the other groups ("Group 1", "Group 2", etc) as needed.
- For each PC you wish to move from the "Everyone" group, enter their details on the *PCs* screen, and assign them to the desired group.

You can limit Internet access for ALL PCs without entering ANY PC data. Simply apply the desired restrictions to the "Everyone" group.

It is also possible to define your own packet filters, and use these filters in addition to the pre-defined filters. Defining your own filters is optional.

Access Control Log

This log is accessed from the *Access Control Log* on the ***Status*** screen. It shows the attempted accesses which have been blocked.

This log can be used to track the operation of the *Access Control* feature. Data shown in this log is as follows:

- **Port** - The port used to gain access to this device. Possible values are LAN, WAN, WLAN (Wireless LAN), and RS232 (serial port).
- **Source IP Address** - The IP Address of the PC or device whose access request was blocked.
- **Physical Address (Hardware Address)** - The hardware address of the PC or device whose access request was blocked.
- **Name** - If known, the name of the device whose access was blocked. This name is taken from the *Access Control* database. For Wireless devices, the name is obtained from the *Wireless Stations* list, and so will always match the Physical (Hardware) address.
- **Destination** - The destination of the attempted access. Possible values are "Internet", "LAN" or "WLAN".
  - "Internet" indicates an outgoing connection attempt which was blocked by the *Access Control* feature.
  - "LAN" or "WLAN" represents an inward connection attempt which was blocked by the Firewall. These inward connection attempts are not affected by the *Access Control* settings.

Security Groups Screen

The *Security Groups* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.

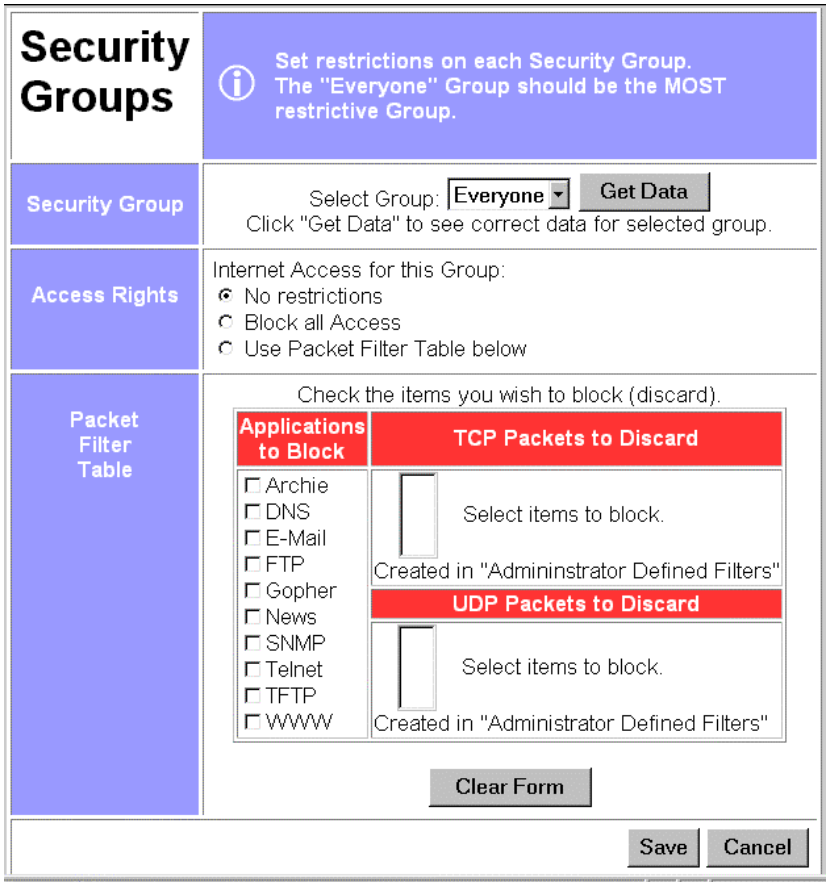


Figure 34: Security Groups Screen

Note that the Security groups are pre-named "Everyone", "Group 1", "Group 2", "Group 3", and "Group 4".

Operations

Define Access Rights for a Security Group

1. Select the group from the drop-down box.
2. Enter the required data as described below.
   If necessary, click *Clear Form* to remove the existing information shown on screen.
3. Click the *Save* button when finished.

Change Access Rights for a Security Group

1. Select the group from the drop-down box,
2. Click *Get Data* to view their information
3. Change any fields you wish.
4. Click *Save* when finished.

Assign PCs to a Security Group

All PCs are initially in the "Everyone" group. Use the *PCs* screen to move individual PCs to other groups as required.

Data – Security Groups Screen

The following data is required.

Access Rights: Internet Access for this Group	
No restrictions	No packets are blocked. Use this to create an "Unlimited Access" group, or to temporarily remove restrictions.
Block all Access	Groups members cannot access the Internet at all. Use this to create the most restrictive group.
Use Packet Filter Table below	Use this to define intermediate levels of access. Using the Packet Filter table gives you fine control over Internet access. Simply select the items you wish to block. You can choose from the pre-defined filters in the *Applications to Block* column, or your own filters in the *TCP Packets to Discard* and *UPD Packets to Discard* column.
Packet Filter Table	
Applications to Block	Any items checked will be blocked. Users will not be able to use the application.
TCP Packets to Discard	This lists any TCP filters you have defined on the *Filters* screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.
UDP Packets to Discard	This lists any UDP filters you have defined on the *Filters* screen. If no filters have been defined, this is empty. Multiple items can be selected (or deselected) by holding down the Ctrl key while selecting items. Selected items can NOT be accessed by members of this group.

If you have not defined your own filters, but wish to do so, refer to "Filters" later in this chapter.

PCs Screen

The *PCs* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.

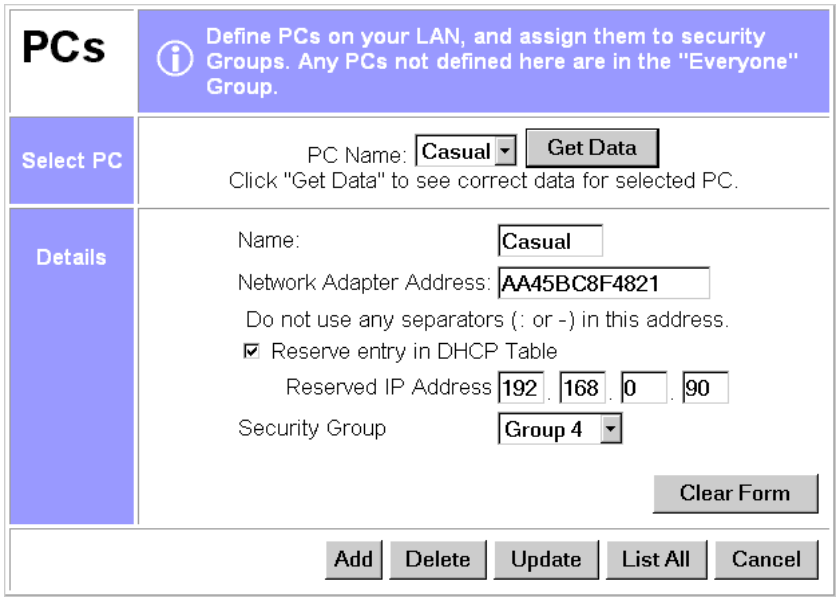

PCs
Define PCs on your LAN, and assign them to security Groups. Any PCs not defined here are in the "Everyone" Group.
Select PC
PC Name: Casual
Get Data
Click "Get Data" to see correct data for selected PC.
Details
Name: Casual
Network Adapter Address: AA45BC8F4821
Do not use any separators (: or -) in this address.
Reserve entry in DHCP Table
Reserved IP Address 192 168 0 90
Security Group Group 4
Clear Form
Add
Delete
Update
List All
Cancel

Figure 35: PCs Screen

Note that the drop-down box lists all PCs previously entered. If none have been entered, this box will be empty.

Operations

Create a new entry

1. Click the "Clear Form" button.
2. Enter the required data, as described below.
3. Click "Add".

Note: The name shown in the drop-down list is ignored.

Delete an entry

1. Select the entry from the drop-down list
2. Click "Delete"

Modify (Edit) an entry

1. Select the entry from the drop-down list.
2. Click "Get Data" to view the current data for this entry.
3. Make any desired changes
4. Click "Update"

Data – PCs Screen

Select PC	
PC Name	This drop-down list shows all entries in the "PC" database. If you have not made any entries, this list will be empty.
Get Data button	Click this button to view the data for the PC selected in the drop-down list. You can then edit the data.

Details	
PC Name	Enter a name to identify this PC.
Network Adapter Address	Hardware address for this PC. You can use the Windows "Winipcfg" program or your LAN management program to find this address.
Reserve entry in DHCP Table	Check this if you wish to reserve an IP address for this PC. This is useful if you have to provide the IP Address for other programs or users. If this is left unchecked, the following entry can be ignored.
Reserved IP Address	This relates to the entry above. Enter the reserved address here. This MUST be within the range used by the DHCP server (set on the *Device - Internal LAN Port* screen).
Security Group	Select the security group for this PC. If you only wish to reserve an IP Address, and are not using the security (access control) features, simply leave this at "Everyone".
Buttons	
Clear Form	Clears all data, ready for input of a new entry.
Add	Add a new entry, using the data shown on screen. The name shown in the drop-down list is ignored.
Delete	Delete the Virtual Server entry selected in the drop-down list, regardless of whether its details are shown on screen.
Update	Update the Virtual Server entry selected in the drop-down list, using the data shown on screen.
List All	List all User-defined Virtual Servers.
Cancel	Reverse any changes made since the last "submit" operation (i.e. since clicking any other button).

Filters Screen

The *Filters* screen is reached from the *Access Control* link on the navigation bar. An example screen is shown below.

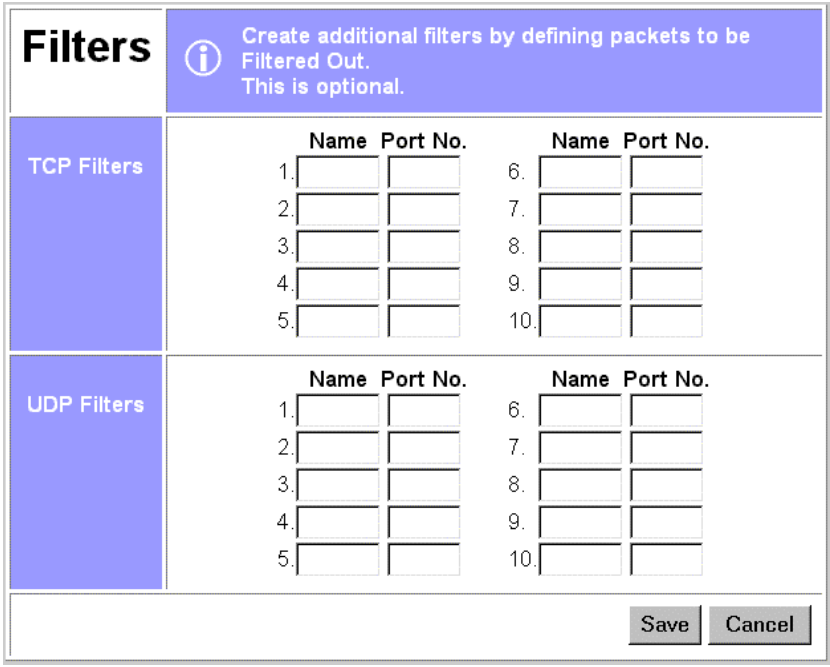


Figure 36: Filters Screen

This screen allows you to define packet filters. When you define security groups, on the "Security Groups" screen, you can select from any filters defined here, as well as the pre-defined filters.

Data – Filters Screen

Define the packets you wish to be filtered out, by entering the following data.

TCP Filters	
Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.
UDP Filters	
Name	Enter a descriptive name for this entry.
Port No.	Enter an integer representing the Port Number for this type of packet. This information can normally be provided by the service provider. Otherwise, a Network Analyzer or Packet Sniffer can be used to determine the correct port number.

Appendix A
Troubleshooting

This Appendix covers the most likely problems and their solutions.

Overview

This chapter covers some common problems that may be encountered while using the Wireless Router and some possible solutions to them. If you follow the suggested steps and the Wireless Router still does not function properly, contact your dealer for further advice.

General Problems

Problem 1: **Can't connect to the Wireless Router to configure it.**

Solution 1: Check the following:

- The Wireless Router is properly installed, LAN connections are OK, and it is powered ON.
- Ensure that your PC and the Wireless Router are on the same network segment. (If you don't have a router, this must be the case.)
- Ensure that your PC is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the Wireless Router's default IP Address of 192.168.0.1.
  Also, the Network Mask should be set to 255.255.255.0 to match the Wireless Router.
  In Windows, you can check these settings by using *Control Panel-Network* to check the *Properties* for the TCP/IP protocol.

Internet Access

Problem 1: **When I enter a URL or IP address I get a time out error.**

Solution 1: A number of things could be causing this. Try the following troubleshooting steps.

- Check if other PCs work. If they do, ensure that your PCs IP settings are correct (IP address, Network Mask, Default gateway and DNS).
- If the PCs are configured correctly, but still not working, check the Wireless Router. Ensure that it is connected and ON. Connect to it and check its settings. (If you can't connect to it, check the LAN and power connections.)
- If the Wireless Router is configured correctly, check your Internet connection (DSL/Cable modem etc) to see that it is working correctly.

Problem 2: **Some applications do not run properly when using the Wireless Router.**

Solution 2: The Wireless Router processes the data passing through it, so it is not transparent.

Use the *Special Applications* feature to allow the use of Internet applications which do not function correctly.

If this does solve the problem you can use the *DMZ* function. This should work with almost every application, but:

- It is a security risk, since the firewall is disabled.
- Only one (1) PC can use this feature.
- When the *DMZ* feature is being used, the *Special Applications* and *Virtual Server* features should be disabled.

Wireless Access

Problem 1: **My PC can't locate the Wireless Access Point.**

Solution 1: Check the following.

- Your PC is set to *Infrastructure Mode*.
- The wireless channel used matches the wireless channel on the Access Point.
- The SSID on your PC and the Wireless Access Point are the same. Remember that the SSID is case-sensitive. So, for example "Work-group" does NOT match "workgroup".
- Both your PC and the Wireless Access Point must have the same setting for WEP. The default setting for the Wireless Router is disabled, so your wireless station should also have WEP disabled.
- If WEP is enabled, the key tables must match.
- If the Wireless Station access permission on the Wireless Router's *Wireless* screen is set to *Only allow access if on this list*, then each Wireless station must have its address correctly entered.
- To see if radio interference is causing a problem, see if connection is possible when close to the Wireless Access Point.
  Remember that the connection range can be as little as 100 feet in poor environments.

Problem 2: **Wireless connection speed is very slow.**

Solution 2: The wireless system will connect at the highest possible speed, depending on the distance and the environment. To obtain the highest possible connection speed, you can experiment with the following:

- Access Point location.
  Try adjusting the location and orientation of the Access Point.
- Wireless Channel
  If interference is the problem, changing to another channel may show a marked improvement.
- Radio Interference
  Other devices may be causing interference. You can experiment by switching other devices Off, and see if this helps. Any "noisy" devices should be shielded or relocated.
- RF Shielding
  Your environment may tend to block transmission between the wireless stations. This will mean high access speed is only possible when close to the Access Point.

Printing

Problem 1: **When I tried to install the Printing software for Peer-to-Peer printing, I received an error message and the installation was aborted.**

Solution 1: This may be caused by an existing installation of the printer port software. Before attempting another installation:

- Remove the existing installation
- Restart your PC

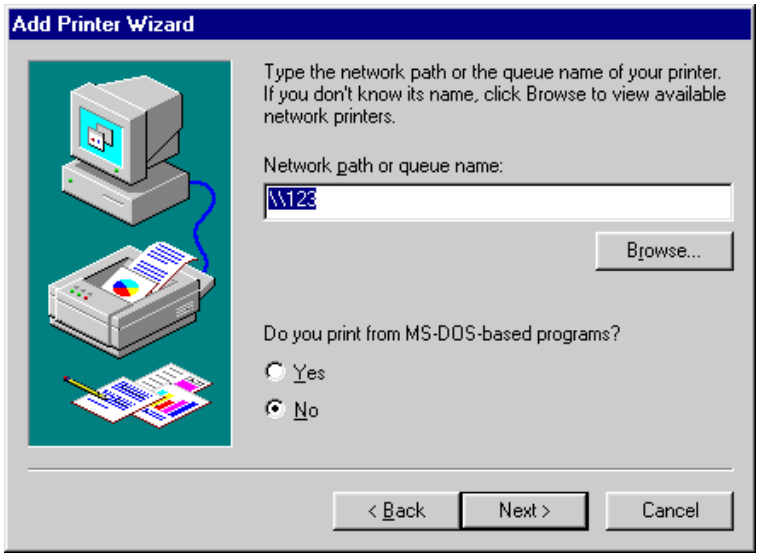
To remove an existing printer port installation:

1. Open Start - Settings - Control Panel - Add/Remove Programs
2. Look for an entry with a name like "Shared Port", "Shared Printer Port", "Print Server Driver" or "Print Server Port".
3. Select this item, click "Add/Remove", and confirm the deletion.

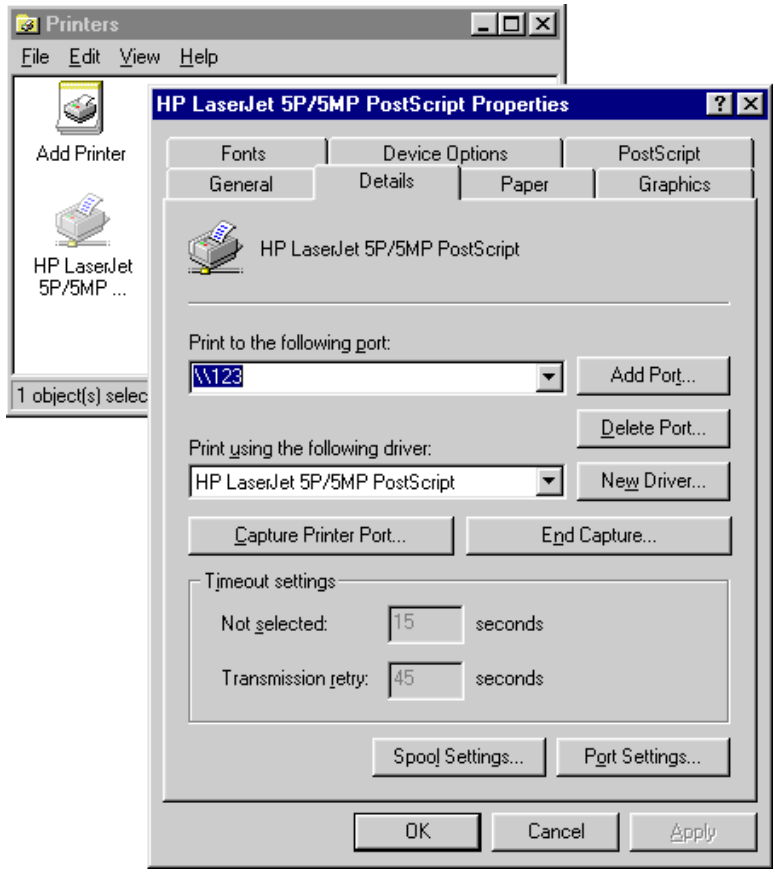
Problem 2: **I am using Windows 95, and the Printing software installed and ran, but when I selected a port and clicked "Add"; the printer was not installed.**

Solution 2: Try installing the printer using the standard Windows tools, as follows:

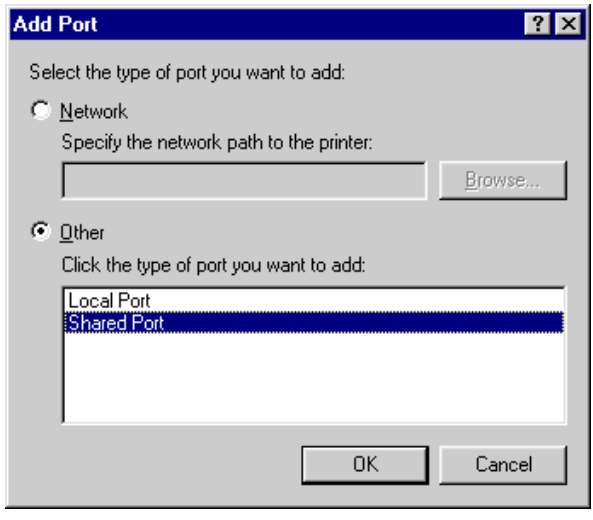
1. Start the *Add Printer* Wizard.
2. Select *Network Printer* when prompted "How is the printer attached to your Computer?", and click Next.
3. When prompted for the Network Path or Queue, enter a dummy value such as \\123, as shown below. (Do NOT select *Yes* for "Do you print for MS-DOS programs?")


Add Printer Wizard
Type the network path or the queue name of your printer. If you don't know its name, click Browse to view available network printers.
Network path or queue name:
\\123
Browse...
Do you print from MS-DOS-based programs?
Yes
No
< Back
Next >
Cancel

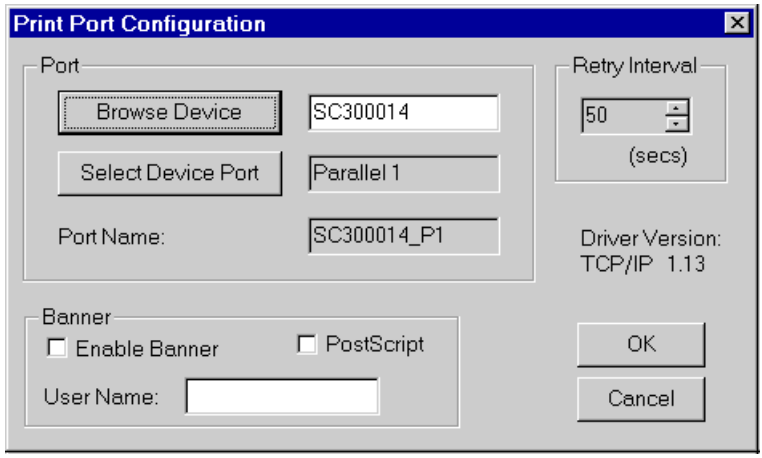
4. The printer wizard will display a message stating that “The Network Printer is off-line”. This is OK. Continue the Add Printer Wizard until finished.
5. When finished, go to *Control Panel-Printers*. The printer icon will be grayed out indicating the printer is not ready.
6. Right-click the Printer, and select *Properties*. Then select the *Details* tab, as shown below.



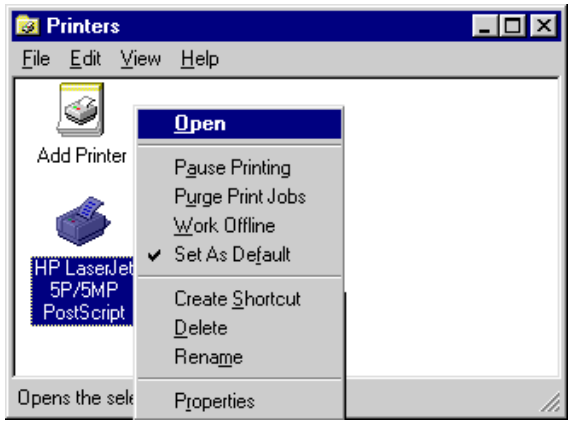
7. Click the *Add Port* button. On the resulting screen, select *Other*, then *Shared Port*, as the port to add, as shown below.



8. Click OK to see the *Print Port Configuration* screen, as shown below.



9. Click the *Browse Device* button, select the desired Wireless Router, and click OK.
10. Click OK to return to the Printers folders, and right-click on the Printer. Ensure that the *Work off-line* option is NOT checked.



The Printer should no longer be grayed out, and is ready for use.

Problem 3: **On my Macintosh, the Wireless Router's printer is not listed.**

Solution 3 Check the following:

- Ensure the network connection is working. If you can connect to the Wireless Router for configuration, then the connection is OK.
- Ensure the *Printer Object Type* on the Wireless Router's *Printer Port* screen is set correctly. If this is wrong, the printer will not be listed on the Macintosh. Check your printer manufacturer's documentation or Web site to determine the correct *Object Type* for your printer.

Dial-in Access

Problem 1: **Remote PC can't connect to the Wireless Router.**

Solution 1: **Check the settings on the Wireless Router**

- Serial Port is Enabled.
- Dial-in is Enabled.
- User has been created, and has Dial-in permission.
- Call-back settings are correct for this user.
- Modem settings are correct.
- Both the Wireless Router and the remote PC are using the same settings for the login authentication (PAP, CHAP, MSCHAP).

Check the Modem

- Modem is properly connected and powered on.
- The modem is working correctly, and the Remote user is dialing the correct telephone number for the modem.
  This can be checked by listening to the modem. You should hear the Wireless Router's modem answer the incoming call.
  - If the call is received but not answered, the modem's "Auto-answer" feature is turned OFF. To turn it on, add the appropriate AT command to the *Initial String* in the on the Wireless Router's *Modem Properties* screen. See Chapter 6 for details of the *Modem Properties* screen, and Appendix C for more information on AT commands.
  - If the call is answered, but no connection is established, then either the modems are unable to negotiate a connection, or the login to the Wireless Router has failed.
    This can be checked by examining the Log file for the Remote PC. See *Finding the current Initial String* in Appendix C for instructions on enabling and viewing the Log file.

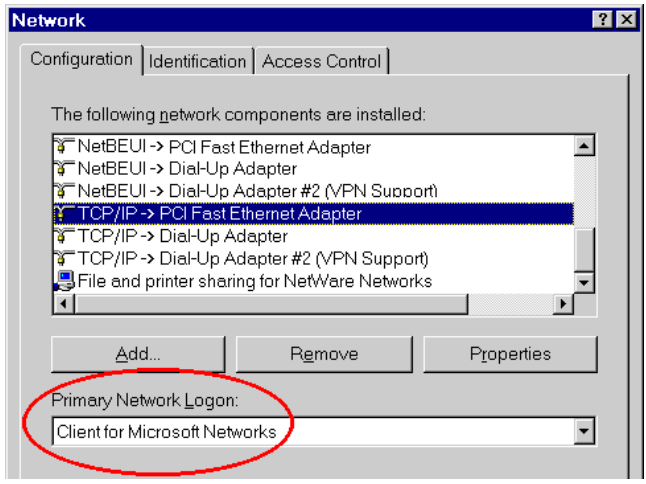
Check the Remote PC

- Ensure that both the Wireless Router and the remote PC are using the same settings for the login authentication (PAP, CHAP, MSCHAP).
- When prompted for "User Name" and "Password", the remote user must enter the correct *User Name* and *Password*, as configured on the Wireless Router's *User Details* screen.
- The modem Log file on the remote PC may provide useful information about the cause of the connection failure. See *Finding the current Initial String* in Appendix C for instructions on enabling and viewing the Log file.

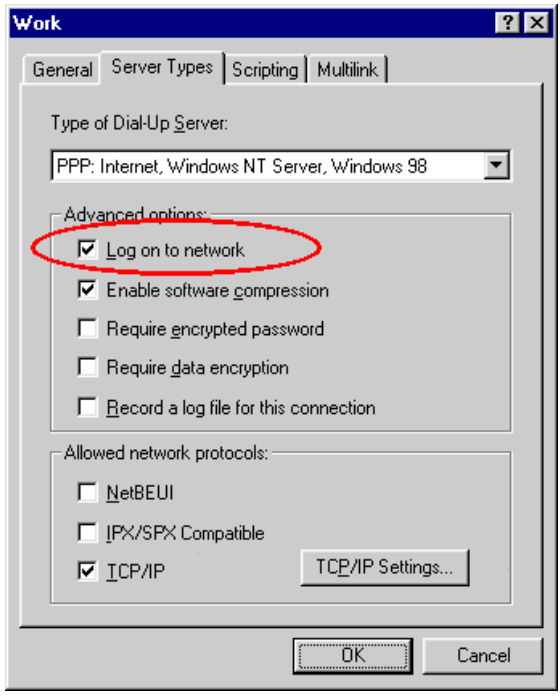
Problem 2: **Remote PC can connect, but can't access LAN resources.**

Answer 2: On the Remote PC, check the following:

- Network Logon is set to "Client for Microsoft Networks", as shown below.
  This screen is reached by using *Start - Settings - Control Panel - Network*.

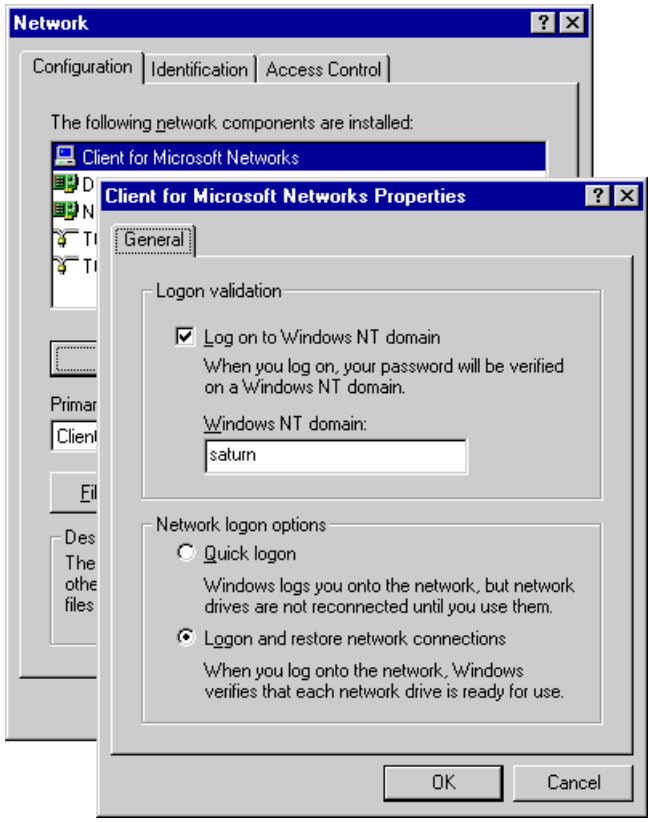


- In the *Properties* for the PPP dial-up connection, the setting "Log-on to Network" is **Enabled**, as shown below.



- If the remote user wishes to logon to a Server after establishing a PPP dial-in connection, the Server login must be configured in the *Properties* for *Client for Microsoft Networks*, as shown below.

  Note:
  This will cause an error message when booting up, because the Server is unavailable. While this can be avoided by only checking the "Log on.." checkbox as required, this change requires restarting your PC.


Network
Configuration
Identification
Access Control
The following network components are installed:
Client for Microsoft Networks
Client for Microsoft Networks Properties
General
Logon validation
Log on to Windows NT domain
When you log on, your password will be verified on a Windows NT domain.
Windows NT domain:
saturn
Network logon options
Quick logon
Windows logs you onto the network, but network drives are not reconnected until you use them.
Logon and restore network connections
When you log onto the network, Windows verifies that each network drive is ready for use.
OK
Cancel

Problem 3: **On the LAN, there is an IP Address conflict involving the Dial-in PC. How do I set the IP Address allocated to the Dial-in PC?**

Answer 3: This problem can only occur if the Wireless Router's DHCP Server is Disabled.

In this situation, the DHCP Server must still allocate an IP Address to the Dial-in user. To set this IP Address:

1. Connect to the Wireless Router
2. On the *Quick Setup* screen, locate the DHCP Server section, and set both the *Start IP Address* and the *Finish IP Address* to the IP Address you wish to be assigned to the Dial-in user.
3. Save these settings.

Appendix B
About Wireless LANs

This Appendix provides some background information about using Wireless LANs (WLANs).

Modes

Wireless LANs can work in either of two (2) modes:

- Ad-hoc
- Infrastructure

Ad-hoc Mode

Ad-hoc mode does not require an Access Point or a wired (Ethernet) LAN. Wireless Stations (e.g. notebook PCs with wireless cards) communicate directly with each other.

Infrastructure Mode

In Infrastructure Mode, one or more Access Points are used to connect Wireless Stations (e.g. Notebook PCs with wireless cards) to a wired (Ethernet) LAN. The Wireless Stations can then access all LAN resources.

Access Points can only function in "Infrastructure" mode, and can communicate only with Wireless Stations which are set to "Infrastructure" mode.

BSS/ESS

BSS

A group of Wireless Stations and a single Access Point, all using the same ID (SSID), form a Basic Service Set (BSS).

Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other.

ESS

A group of Wireless Stations, and multiple Access Points, all using the same ID (ESSID), form an Extended Service Set (ESS).

Different Access Points within an ESS can use different Channels. In fact, to reduce interference, it is recommended that adjacent Access Points SHOULD use different channels.

As Wireless Stations are physically moved through the area covered by an ESS, they will automatically change to the Access Point which has the least interference or best performance. This capability is called **Roaming**. (Access Points do not have or require Roaming capabilities.)

Channels

The Wireless Channel sets the radio frequency used for communication.

- Access Points use a fixed Channel. You can select the Channel used. This allows you to choose a Channel which provides the least interference and best performance. In the USA and Canada, 11 channel are available.
- Client (PC) Wireless Stations normally scan all Channels, looking for an Access Point. If more than one Access Point can be used, the one with the strongest signal is used. (This can only happen within an ESS.)
- If your PC's wireless card does NOT automatically scan all wireless channels, then you must manually set it to the Channel used on the Access Point.

WEP

WEP (Wired Equivalent Privacy) is a standard for encrypting data before it is transmitted.

This is desirable because it is impossible to prevent snoopers from receiving any data which is transmitted by your Wireless Stations. But if the data is encrypted, then it is meaningless unless the receiver can decrypt it.

If WEP is used, the Wireless Stations and the Access Point must have the same settings for each of the following:

WEP	Off, 64 Bit, 128 Bit
Key	For 64 Bit encryption, the Key Table must match. For 128 Bit encryption, the Key value must match.
WEP Authentication	Open System or Shared Key.

Access Control

The *Access Control* feature allows you to determine which Wireless Stations can use the Access Point. You need to identify each Wireless Station by its Hardware or physical Address.

On Windows, you can determine the Hardware (physical) Address using *WinIPCfg*, as follows:

1. Use *Start* - *Run* to open the "Run" dialog.
2. Type `WINIPCFG` and press Enter (or click OK).

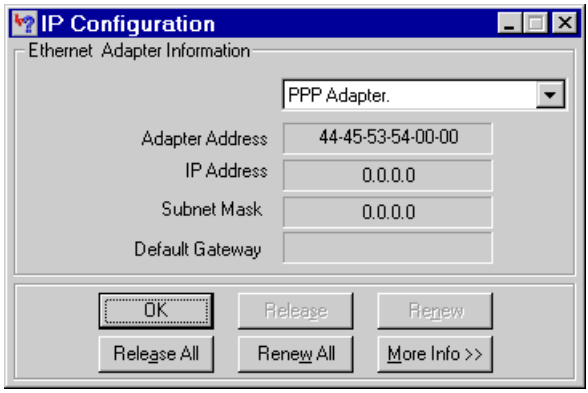


Figure 37: WinIpCfg

3. WinIPCfg will then run, as shown above.
4. Select your Wireless adapter from the drop-down list, and check the *Adapter Address* field.

Wireless LAN Configuration

To allow Wireless Stations to use the Access Point, the Wireless Stations and the Access Point must use the same settings, as follows:

Mode	On client Wireless Stations, the mode must be set to "Infrastructure". (The Access Point is always in "Infrastructure" mode.)
SSID (ESSID)	Wireless Stations must use the same SSID (ESSID) as the Access Point they wish to connect to.
WEP	The Wireless Stations and the Access Point must use the same settings for WEP (Off, 64 Bit, or 128 Bit). **WEP Key:** If WEP is enabled, the Key Table (for 64 Bit encryption) or Key (for 128 Bit Encryption) must be the same on the Wireless Stations and the Access Point. **WEP Authentication:** If WEP is enabled, all Wireless Stations must use the same setting as the Access Point (either "Open System" or "Shared Key").

Appendix C
AT Commands

AT Commands

This Appendix details the "AT" commands used by modems and ISDN TAs. This information is provided to assist users who are using the Wireless Router's serial (RS232 port).

It is not relevant to Cable or DSL modems connected to the WAN (Ethernet) port.

Required Settings

For the Wireless Router to use the Serial Port correctly, the modem or ISDN TA must be set as follows.

Setting	AT Command
Fixed baud rate setting	AT&B1
RTS/CTS flow control	AT&K3
DCD to track the presence of a carrier	AT&C1
DTR off to hang-up modem	AT&D2
DSR always on	AT&S0

If your Modem or ISDN TA uses the commands above, then the *Initial String* would be as follows:

```
AT&F&B1&K3&C1&D2&S0X4
```

Notes:

- The command "AT&F" is used to set the modem to the factory default settings, to ensure a consistent starting point.
- For some Mircocom and other modems, the "ATX4" command is not sufficient - a "W2" command (no "AT") must be used as well.
- ISDN TAs may not use these commands; please check your user guide for your ISDN TA.

Finding the current Initial String

If your modem or ISDN TA is already working correctly using the PC's serial port, but you don't know what the initialization string is, you can use the following procedure to find out.

1. Select *My Computer*, then *Dial-Up Networking*.
2. Select the icon for your connection, then *Properties*.
3. Click the *Configure* button, then the *Connection* tab, as shown below.

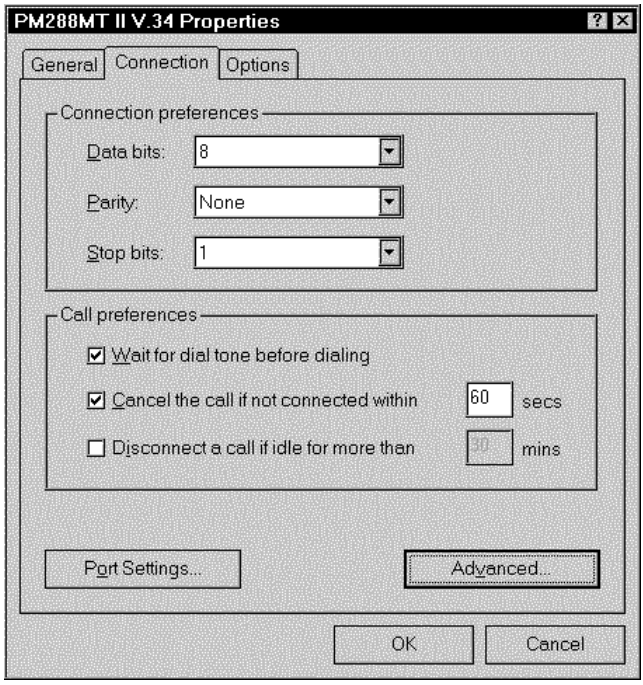


Figure 38: Connection Properties (W95/98)

4. Select *Advanced* to see the screen below.

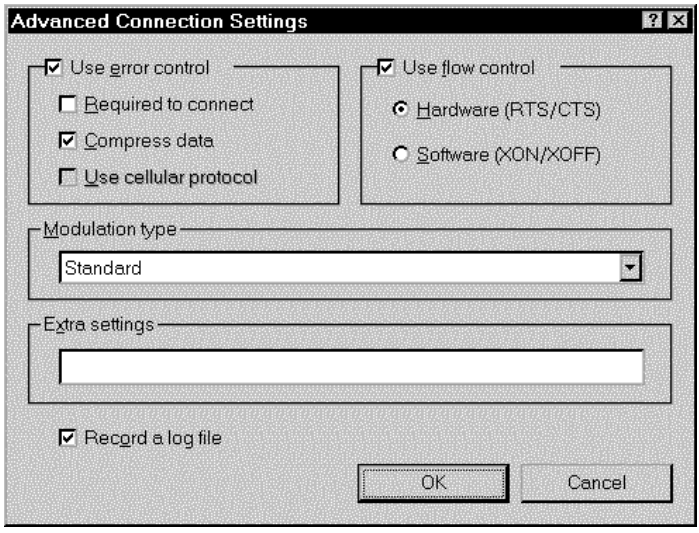


Figure 39: Advanced Connection (W95/98)

5. Check the option *Record a log file*. Then click *OK* and exit.
6. Use *Dial-up Networking* to make your on-line connection normally. A log file MODEMLOG.TXT will be created in your Windows directory.
7. Use Notepad or another editor to read and print the file MODEMLOG.TXT.
8. Examine the file to determine the *Initial String* value. It will be near the beginning of the file, and look something like the example shown previously.

Standard AT Commands

Most modems use the standard AT commands, as shown in the following tables. Consult the manual for your modem to set what AT commands it supports.

Note that the trailing "n" in many commands indicates a number.
The allowable numbers, and their effect, are listed below the command.

Command		Description
<any key>		Terminate current connection attempt
+++		Escape sequence code, entered in data state, wait for modem to return to command state
ATA		Force answer mode on-line
ATEn		Handshake operation
	B0	Select ITU-T V.22 for 1200 bps communication
	B1	Select Bell 212A for 1200 bps communication
ATD		Dial number and options that follow
	P	Pulse dial
	T	Tone dial
	,	Pause for a specified time
	;	Return to command state after dialing
	!	Hook flash, call transfer
	W	Wait for second dial tone
	@	Wait for 5-second silence before proceeding, otherwise return O ANSWER"
	R	Reverse Dial (Originate a call in answer mode)
ATDL		Dial last number
ATDSn		Dial number stored in NVRAM at position *n*. (n=0..9)
ATEn		Command mode local echo of keyboard commands
	E0	Echo off
	E1	Echo on
ATHn		On/Off hook control
	H	Hang up modem
	H0	Hang up (on hook), same as ATH
	H1	Get off hook
ATIn		Display inquired information
	I0	Display product code
	I1	Display product information and ROM checksum
	I2	Link status report

ATLn		Speaker volume control. n=0-7
ATMn		Speaker control
	M0	Speaker always off
	M1	Speaker on until carrier is detected
	M2	Speaker always on
	M3	Speaker on after last digit dialed, off at carrier detect
ATNn		Ring volume control, *n*=0 disables ring function. (n=0..7)
ATO		Return to on-line state
ATP		Pulse dial
ATQn		Result code displayed
	Q0	Modem returns result code
	Q1	Modem does not return result code
	Q2	Return result code but quiet in answer mode (will not show in AT&V*n*)
ATS0=n		Number of rings required before modem answers. n=0 disables auto-answer.
ATSr.b=n		Set bit *b* of S-register *r* to *n*. (n=0 or 1)
ATSr.b?		Inquiry bit *b* of S-register *r*
ATSr=n		Set S-register *r* to value *n*, where *n* is a decimal number between 0-255
ATSr?		Display value stored in S-register *r*
ATT		Tone dial
ATVn		Verbal/Numeric result codes
	V0	Display result codes in numeric form
	V1	Display result codes in verbose form
ATXn		Result code options. (n=0..7)
ATZn		Reset the modem and set power-on profile. (n=0..4)
	Zn	Reset modem and load user profile *n* (n=0..3)
	Z4	Reset modem and load factory settings
AT$		Help, Basic command summary
AT&$		Help, Extended AT& command summary
AT*$		Help, Extended AT* command summary

Extended "AT&" Commands

(Includes RTS/CTS Flow Control Commands)

Command		Description
&Bn		Data rate, terminal-to-modem
	&B1	DTE/DCE rate fixed at DTE setting
&Cn		Carrier Detect operations
	&C1	Carrier Detect tracks presence of carrier
&Dn		Data Terminal Ready (DTR) operations
	&D2	DTR off causes modem to hang up
&F		Load the default factory settings,
&Kn		Data flow control, DTE/DCE, n=0,3,4
	&K0	Flow control disabled
	&K3	Hardware (RTS/CTS) flow control
	&K4	Software (XON/XOFF) flow control
&Sn		Data Set Ready (DSR)
	&S0	DSR overridden, DSR always on

Appendix D
Specifications

Multi-Function Wireless Router

Model	Wireless Router
Dimensions	240mm(W) * 120mm(D) * 35mm(H)
Operating Temperature	0° C to 40° C
Storage Temperature	-10° C to 70° C
Network Protocol:	TCP/IP
Network Interface:	3 Ethernet: 2 * 10/100BaseT (RJ45) for LAN 1 * 10BaseT (RJ45) for WAN
PCMCIA Slot	1 Type II, 16bit bus
Wireless interface	Wireless Access Point via supplied PCMPIA card IEEE 802.11b compatible, WEP security support, roaming support
Printer Port	1 * parallel printer port
Serial Port	1 * RS232 9 pin male port
LEDs	9
Power Adapter	12 V DC External

FCC Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference received, including interference that may cause undesired operation.

CE Marking Warning

This is a Class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

PCMCIA Wireless Card

Interface	PCMCIA 68pin, 16bit data
Standards	IEEE802.11b WLAN, PCMCIA 2.1, JEIDA 4.2
Frequency	2.4 to 2.4835GHz (Industrial Scientific Medical Band)
Channels	Maximum 14 Channels, depending on regulatory authorities
Data Rate	11 / 5.5 / 2 / 1 Mbps
Coverage Area	Closed Space : 25m @11Mbps, 100m @5.5Mbps or lower
Power	DC +3.3V / 220mA
Output Power	13dBm (typical)
Receiver Sensitivity	-80dBm Min.
Operating Temperature	0^{o} to 55^{o}C
Storage Temperature	-25^{o} to 70^{o}C
Relative humidity	10% to 90%